
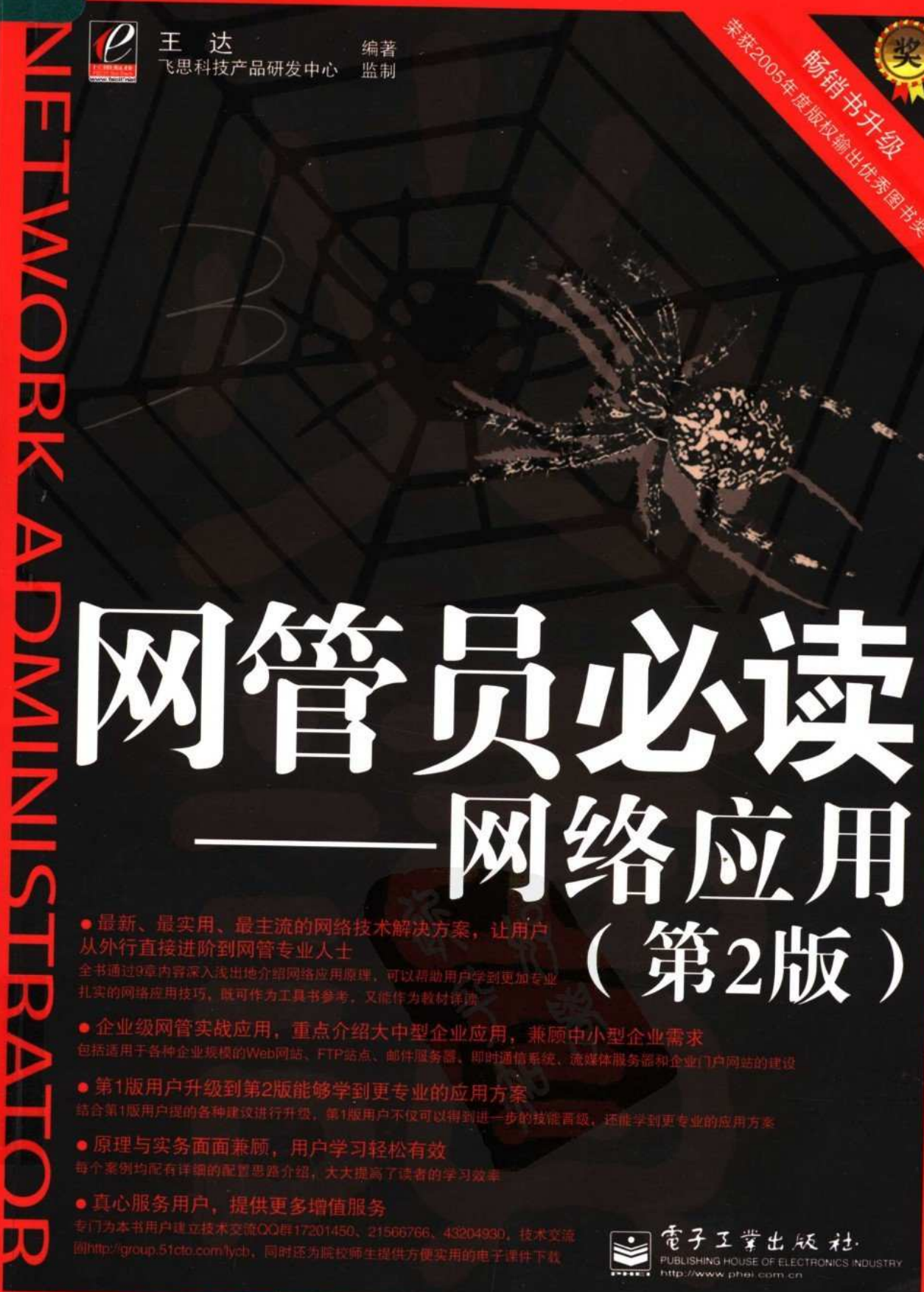


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



王 达
飞思科技产品研发中心

编著
监制

荣获2005年度版权输出优秀图书奖

畅销书升级


NETWORK ADMINISTRATOR

网管员必读

——网络应用

（第2版）

- 最新、最实用、最主流的网络技术解决方案，让用户从外行直接进阶到网管专业人士
全书通过9章内容深入浅出地介绍网络应用原理，可以帮助用户学到更加专业扎实的网络应用技巧，既可作为工具书参考，又能作为教材详读
- 企业级网管实战应用，重点介绍大中型企业应用，兼顾中小型企业需求
包括适用于各种企业规模的Web网站、FTP站点、邮件服务器、即时通信系统、流媒体服务器和企业门户网站的建设
- 第1版用户升级到第2版能够学到更专业的应用方案
结合第1版用户提的各种建议进行升级，第1版用户不仅可以得到进一步的技能晋级，还能学到更专业的应用方案
- 原理与实务面面兼顾，用户学习轻松有效
每个案例均配有详细的配置思路介绍，大大提高了读者的学习效率
- 真心服务用户，提供更多增值服务
专门为本书用户建立技术交流QQ群17201450、21566766、43204930，技术交流
圈<http://group.51cto.com/lycb>，同时还为院校师生提供方便实用的电子课件下载



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“网管员必读”系列为网管员精心打造 职业塑身计划



网管员必读（第1版）



网管员必读（第2版）

上架提示：网络

飞思在线：<http://www.fecit.com.cn>
飞思科技产品研发中心总策划



责任编辑：王树伟
责任美编：李春瑞



本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

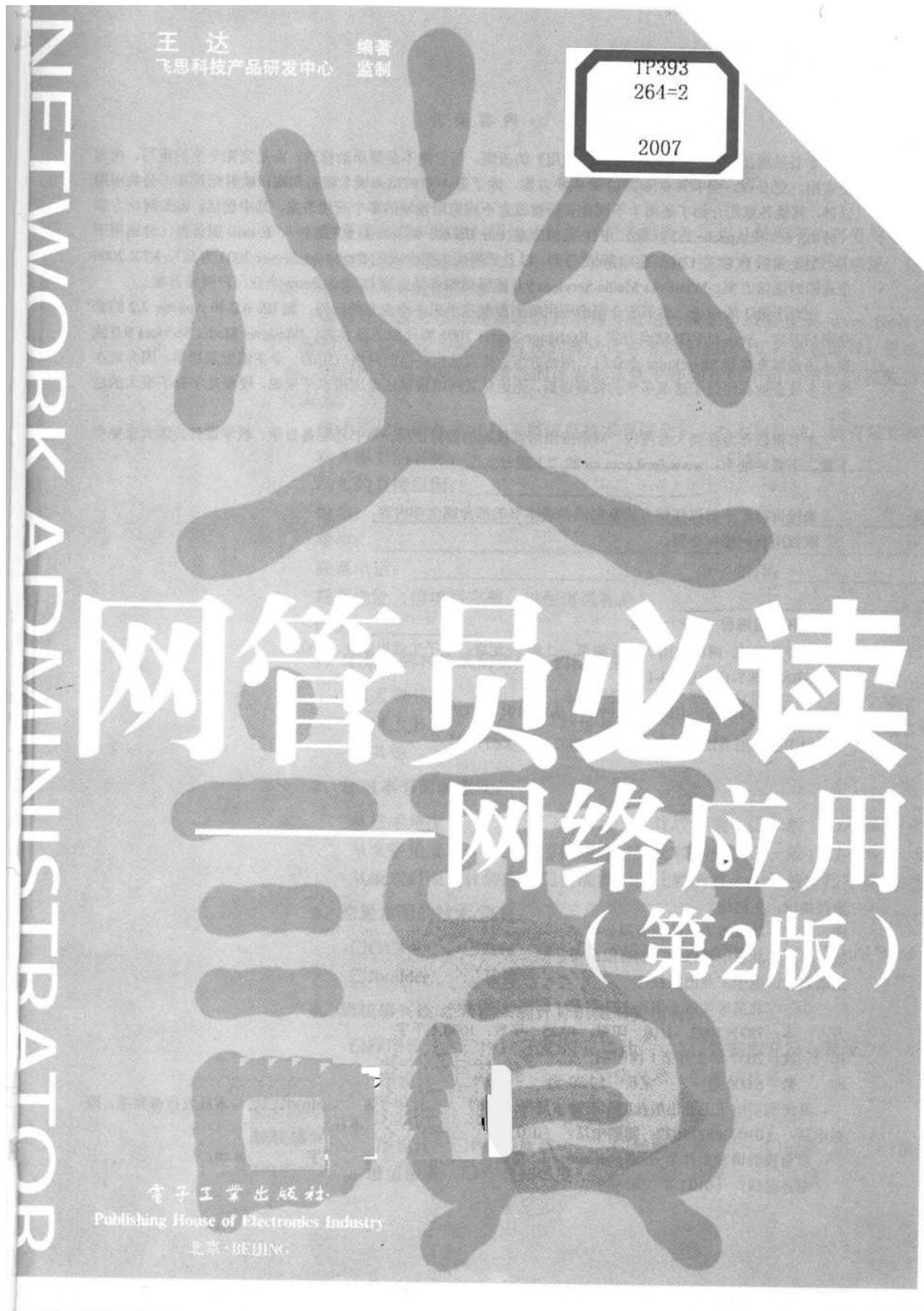
ISBN 978-7-121-03793-1



9 787121 037931 >

定价：59.80元

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

FOREWORD

再版序言

自 2004 年 9 月，《网管员必读》系列丛书第一本、第二本上市之后，以全新的策划视角和系统、专业、深入、实用的内容，使“网管员必读”这五个字深深地融入了千万读者的心中，畅销至今。“网管员必读”成为了 21 世纪初叶网管类图书的金字招牌。

本丛书所取得的成绩和荣誉相信许多读者都有所耳闻。笔者的博客和网络书评记载了本书的成长历程：华储网举办的 2004 年、2005 年度最喜爱的图书评选和第二届书店 2005 年度最权威图书活动，这套丛书均全面上榜，有些排名还非常靠前；2006 年 8 月举办的第十三届国际图书博览会，获得 2005 年度输出优秀图书奖；2006 年 11 月份，在由中国书刊发行业协会组织举办的“2006 年度全行业优秀畅销品种”评选中，该套丛书中的《网管员必读——超级网管经验谈》获得了“2006 年度全行业优秀畅销品种”称号；等等。这些成绩的取得，与广大读者、院校客户、媒体和书店的支持是分不开的。

再版的慎重考虑

基于丛书成绩的取得和千千万万读者的期待，《网管员必读》系列丛书的第 2 版编写计划就实实在在地提到了出版社和笔者面前。“第 1 版的优异成绩，决定了第 2 版只能更好。”这是出版社和笔者共同的决心。为此，对第 2 版的编写，出版社和笔者用足了心血，一次又一次地讨论和修改再版方案，不仅在内部进行，还专门请相关专家进行方案评审。在两年多再版方案的讨论中，无数读者通过各种方式提出了宝贵的修改意见。在此，我们表示由衷的感谢！

由于第 1 版图书已有较大影响，不仅终端读者希望选用这套书系统地学习，就连高等院校和培训机构也希望采用这套丛书作为教学、培训的教材，还有许多想参加国家计算机软件水平考试（简称“软考”）的读者也希望通过这套丛书顺利通过“网络管理员”考试。我们深感重任在身，必须尽心尽力，极为慎重地对待本次改版工作。

新版丛书的内容调整

经过再三讨论和修改后，最终的再版方案终于出炉了。主要在以下几个方面进行了修订。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1. 重新调整了丛书内容

第1版由于各种原因，有部分选题或者内容存在着重复现象。当然，这不是笔者故意所致，而是受出版计划的影响。在第2版中，笔者针对这一现象，对各本书的内容做了重大调整，全面避免了选题、内容上的交叉重复，进一步提高了图书的实用性和内容之间的关联性。这一改变相信大家可以从新版图书目录中管中窥豹，可见一斑。

2. 新增了大量新技术和新应用案例

自第1版丛书出版两年来，网络技术和应用出现了比较大的发展。为了充分体现时代特色，满足读者学习和掌握新技术、新应用的需求，同时考虑到读者实际需求，新版中均添加了大量新的网络技术和应用方案。如《网管员必读——网络基础》一书的博客、RSS、Wiki、SNS，以及新的交换机和路由器技术等；《网管员必读——网络应用》一书中的 Windows Media Service 9.0、Live Communications Server 2005 和 SharePoint Portal Server 2003 等应用；针对网络管理员“软考”大纲要求，在《网管员必读——网络基础》一书中专用两章增加了“数制”和“网络通信基础”等方面的内容。新内容新案例的添加，使新版图书更加贴近了网络管理员“软考”大纲的要求。

3. 全面采用最新软件系统版本

新版中，凡是涉及到操作系统和应用软件，均改为最新版本，以便让读者全面掌握新技术和新产品带来的优势。如《网管员必读——网络管理》一书中的 Windows Server 2003 系统改为 R2 版本，原来的 RedHat Linux 9.0 改为 RedHat Enterprise Linux 4.0；《网管员必读——网络应用》中的各种应用软件都同样全面采用最新版本，特别是原来的 Exchange 2000 Server，现改为 Exchange Server 2003。

4. 全面审订原书中的不妥之处

任何图书由于各种原因会存在一些错误或者不妥之处，第1版《网管员必读》系列丛书也不例外，已发现的错误和不妥之处都在第2版中得到全面修订，有的地方改动较多。如对《网管员必读——网络基础》原书中的几章（“IP 协议”、“局域网基础”）内容在新版中做了重新编写。对于全面采用新版软件的图书，如《网管员必读——网络应用》、《网管员必读——网络管理》和《网管员必读——超级网管经验谈》这3本书的重写内容，达到了80%以上。

5. 替换了所有不完美的图片

在第1版中，有读者和同行反映，自画图片质量较差，经查的确如此。因为在编写第1版丛书的前两本图书时笔者手中并没有专业的拓扑结构或者图片绘制软件，所以绘制的图片质量较差，影响阅读效果。不过自《网管员必读——超级网管经验谈》一书后基本上不存在这个问题了。在新版中，已对这些图片进行了全面替换，均采用专业的绘图工进行绘制，使图片质量有了较大幅度的提升。

6. 增加《网管员必读——网络术语词典》和《网管员必读——网络测试与实验》两本书

这两本书是应广大读者建议而增加的。《网管员必读——网络术语词典》一书比较全面地把当前主流应用的网络技术，包括局域网、广域网基础和网络存储等术语包含其中。《网

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

管员必读——网络测试与实验》这本书侧重于网络线路和性能的测试，各种主流虚拟服务器、虚拟客户端系统配置与使用，以及主要品牌网络设备模拟器的配置与使用等方面。这样，该套丛书由 10 册组成，与笔者正在编写并陆续出版的《网络工程师必读》系列丛书形成姊妹篇。

7. 全面增加课件内容

为了便于读者自学和老师教学（在第 1 版中就有不少高等院校老师专门请作者为他们编写了课件），新版图书全面增加了文字版的 PPT 教学课件（特别适合于老师教学使用）。PPT 课件全部放在飞思网站（www.fecit.com.cn）上免费供读者和老师下载使用。

新版主要特色和亮点

说到新版丛书的特点和亮点，作为这套书的作者着实非常兴奋。因为我们从这套新版丛书的修改方案中看到了非常多的新特色和新亮点。出版社和笔者都对这套新版丛书的前景充满了自信。新版丛书的主要特色和亮点如下。

1. 内容更丰富、更实用

新版丛书在第 1 版的基础上增加了大量新的技术和新的应用内容，既充分体现了时代特色，又实实在在地让读者领略到新技术所带来的实惠。再加上新版丛书中增加了两种 PPT 课件，使读者学习、老师教学更加方便，进一步提高了丛书的实用性。

2. 结构更严谨、更系统

新版丛书将第 1 版中的重复选题、重复内容全部重新整合，使得整套丛书结构更加严谨、系统性更强。另外，在编写新版丛书时，对原书中的许多过时、叙述不妥当的内容进行了修改，甚至重写，使得新版丛书的新内容更丰富，专业性更强。

3. 更方便自学和教学

在新版本中，突出重点与难点，特别是在网络组建、网络应用等方面，突出强调了网络技术学习、应用方案配置的整体思路。这样就可以使读者及使用本书作为教材的用户全面系统地进行学习。

4. 更多专业、实用的经验和技巧

通过几年来与广大读者的交流，我们更充分地了解了各种类型读者的真正需求，同时也积累了许多专业、实用的经验与技巧。这些积累都将在第 2 版的图书中得到全面体现。其中包括许多在第 1 版中读者向笔者问的问题解答，这些问题都具有一定的代表性，可以帮助读者解决实际工作中遇到的问题。

5. 自学、教学和软考三不误

新版丛书在编写之时就对读者自学、老师教学和参加计算机软件（水平）考试这三方面的需求做了充分考虑，所以在具体内容组织和安排上全面满足了这三方面的需求。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

丛书使用建议

本套新版丛书各本中的内容都有一定的关联性，逻辑性十分严密。如果您原来没有系统地学习过网络管理知识，建议全套购买，这样学习效果最好。这在第1版中已得到了广大读者的证明，因为这是目前市面上唯一一套如此系统的网络管理类丛书，十分适合广大读者自学使用。

建议学习本套丛书顺序如下：《网管员必读——网络基础》→《网管员必读——网络组建》→《网管员必读——网络测试与实验》→《网管员必读——网络应用》→《网管员必读——网络管理》→《网管员必读——网络安全》→《网管员必读——超级网管经验谈》→《网管员必读——服务器与数据存储》。《网管员必读——故障排除》和《网管员必读——网络术语词典》两书属于工具类参考图书，可在需要时即时查阅。

另外，对于想参加网络工程师软考的读者朋友，可以同时选择笔者编著的《网络工程师必读》系列。在学习《网管员必读——网络基础》一书时请结合《网络工程师必读——网络工程基础》、《网络工程师必读——接入网与交换网》两书一起学习；在学习《网管员必读——网络组建》一书时，请结合《网络工程师必读——网络系统设计》、《网络工程师必读——综合布线》和《网络工程师必读——网络设备配置与管理》、《网络工程师必读——虚拟专用网》、《网络工程师必读——无盘网络》这五本书一起学习；在学习《网管员必读——网络安全》一书时请结合《网络工程师必读——网络安全系统设计》一书一起学习；在学习《网管员必读——服务器与数据存储》一书时请结合《网络工程师必读——网络存储》一书一起学习。

最后，要充分利用我们所提供的PPT课件，实现自学、教学效果的最佳化。当然，老师可以根据本校学员的实际情况对教学课件进行各种修改。

编 著 者

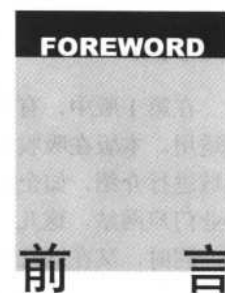
联系方式

咨询电话：(010) 68134545 88254160

电子邮件：support@fecit.com.cn

服务网址：<http://www.fecit.com.cn> <http://www.fecit.net>

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT



随着近十年来网络应用的发展，企业网络应用水平也在不断提高，不再满足于那些小而简单的共享软件所提供的功能，更趋于专业化的道路。正是在这一背景下，笔者提出了对《网管员必读——网络应用》全面改版的要求，在得到电子工业出版社北京易飞思信息技术有限公司领导的支持下，对第1版的内容进行重组优化，删除了原来一些比较少用的应用方案，增加了大量适用于大中型企业的网络应用方案，如 Exchange Server 2003 邮件服务器方案、Windows Media Service 流媒体方案、SharePoint 企业门户网站方案等。对第1版图书中保留的内容，也都全面进行了软件版本升级，新增了近年来笔者积累的大量方案应用经验和故障排除经验，使得本版图书内容更加专业、更加实用。相对于第1版来说，本版图书的特色更加鲜明，具体如下。

优化重组

即使是同样的选题内容，如 IIS 网站、Apache 网站、Serv-U FTP 站点、CMail 和 Exchange 邮件服务器等，本书都对软件版本进行了更新。因为距第1版时间（第1版上市时间为2004年9月）较长，所以软件版本改变了许多，相应功能也有了许多改变，这样就不得不重新组织。

当然，优化重组不仅体现在对原来保留的选题进行重写，还新增了一些应用方案，如第1章的动态域名解析和端口映射，这可是当前网络应用的热点，还有如 Windows Media Service 流媒体服务器、SharePoint 企业门户网站也都是新增加的。使得整个图书的内容更充实、更实用。

更加专业

这一点在前面已有提到。因为本书介绍了大量适用于大中型企业的复杂应用方案，如 Exchange Server 2003 邮件服务器方案、Windows Media Services 流媒体方案、SharePoint 企业门户网站方案等，所以本书尽管所介绍的方案数量比第1版少，但篇幅却有大幅度提升。因为在其中有几章，单一方案的篇幅都达到了100页以上。之所以如此细致地介绍，其目的就是想全面而又系统地介绍这些复杂应用的各主要方面，让读者能比较深入地掌握一些高级应用配置，而不是只停留在肤浅的表面应用。这一点在大中型企业中尤为重要。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

更加实用

在第1版中，有读者认为书中的有些内容不够深入，对一些高级的网络管理员来说不是很适用。本版在吸收这些读者意见的基础上，对方案做了重大调整，只选取最为主流的应用领域进行介绍，如企业 Web 网站、FTP 站点、邮件服务器、即时通信平台、流媒体服务器和企业门户网站。这几个领域是目前企业网络应用的最主要领域。

同时，又在这几个主要应用领域中进行细分，尽可能在最大限度满足大中型企业的专业应用的基础上，照顾到仍在中小型企业担当网络管理的朋友的需求，对一些常见领域提供了适用于中小型企业的相应方案，这样就可以比较全面地满足各类档次的读者需求。新读者可以从中吸收更多应用方案的配置知识，老读者也可以从中得到自己水平提高后所需的高级应用方案配置知识。

当然，由于篇幅的限制，有些方案的配置还不能介绍得很全面，而且企业网络应用方案也远不止这些，在此只能对大家说对不起了。有些比较小型的应用将在本系列丛书的《网管员必读——超级网管经验谈》和《网管员必读——网络原理》两书中介绍，敬请留意笔者博客（<http://blog.51cto.com/blog.php?uid=55153>）中的最新图书资讯，也可加入3个专门的QQ读者群：17201450、21566766、43204930。

本书由王达主笔并统稿，参加编写、校对和排版的人员有：何艳辉、王珂、沈芝兰、马平、何江林、刘凤竹、卢京华、周志雄、洪武、高平复、周建辉、孔平、尚宝宏、姚学军、刘学、李翔、王娇、李敏、吴鹏飞等，在此一并由衷地感谢。由于编者水平有限，尽管我们花了大量时间和精力校对，但书中可能还存在一些错误，敬请各位批评指正，万分感谢！

编 著 者

联系方式

咨询电话：(010) 68134545 88254160

电子邮件：support@fecit.com.cn

服务网址：<http://www.fecit.com.cn> <http://www.fecit.net>

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

FOREWORD

编辑的话

在从事图书出版这十年间，得以结识很多优秀作者，并和他们成为相互信任的朋友，这成为我十年来最可宝贵的财富。王达老师是这些优秀作者中很突出的一位。

2002年，我们以邮件方式相识，并在选题切磋的过程中彼此了解，进而产生了初步的信任，但王达老师与我们真正的合作是从2004年《网管员必读》系列丛书开始的。

《网管员必读》系列丛书经过两年多的市场考验，以其专业性和实用性取得了读者的信任。与此同时，该系列图书的品质不仅为中国大陆市场接受，也获得了中国台湾地区出版界的认可。《网管员必读》系列丛书荣获“2005年度输出优秀图书奖”，其中部分图书入选“2006年度全行业优秀畅销品种”。这一系列图书何以获得图书市场的认可呢？在《网管员必读》系列丛书第2版全新登场之际，我们愿意和广大读者共同分享背后的故事。

《网管员必读》系列丛书是飞思“产品全程策划+品牌营销的项目化运作”策划理念的典型案例。任何一个产品都要经历从无到有，从成长到发展这样一个过程。图书也有生命周期，有其策划、产生、成熟和发展的过程。这一系列图书的成功是《网管员必读》项目组共同努力的结果。我们建立了以策划人员为首的，包括作者、市场人员、技术编辑、美术编辑等关键岗位人员共同组成的项目组，对“网管员必读”系列品牌进行培育。

精心策划

在产品的导入期，因为《网管员必读》系列丛书是图书出版市场上第一套以网管员职业为切入点，横向剖析网管员专业的技术图书，它存在着市场风险，即这种体系的规划方式是否能够被读者接受。于是，我们与业内人士进行了深入的探讨，包括当时在《网管员世界》杂志任主编、现在是51cto网站内容总监的杨文飞老师，新科海培训学校的孙亚刚校长，以及一些网络公司的工程师等。同时，在网上以调查问卷的形式对本丛书的内容体系结构进行了广泛的意见征集。在此基础上，初步形成了以目标用户需求为导向的调查问卷。为广泛了解读者对网管员职业的要求，以及培训学校对网管员职业培训结构的要求，项目组又选择互动出版网、几家网管员活跃的论坛作为网络调研的平台，进行了几个月的充分调研（如右图所示）。综合各方面的意见后，我们完善了本系列丛书的体系架构，为丛书作者写作打下了坚实的基础。

网管员职业培训需求调查

- 您认为网管员的职责：
☐ 网络维护 ☐ 网络故障排除 ☐ 专业报刊杂志 ☐ 大型期刊杂志 ☐ 校园网建设
- 您希望增加的培训内容：
☐ 网络安全 ☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 其他
- 您希望增加的培训方法：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您希望增加的培训教材：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品
- 您认为网管员的培训需求：
☐ 网络维护 ☐ 网络故障排除 ☐ 网络管理 ☐ 网络应用 ☐ 网络产品

互动出版网的网上调查问卷

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

精心制作

当图书进入编辑加工生产阶段，《网管员必读》项目组虚心听取专业人士的意见，邀请业界专家加入到图书技术审校工作中来，并把专家的意见、建议及编辑人员在书稿加工过程中发现的问题及时反馈给作者，使图书品质得到了进一步的提升。在图书整体装帧设计上，我们也专门针对“必读”二字进行系列整体品牌认知标识的设计，使丛书的整体冲击感及给读者的认知感得到了很大的提升。

精心宣传

在“好酒也怕巷子深”的年代，为了让广大网管人员及时了解本丛书的出版信息，我们在《网管员必读》系列丛书的宣传和传播上也做了精心的部署。从2004年《网管员必读》系列图书的第一本上市至今两年多的时间里，我们开展了一浪接一浪的宣传活动。在图书上市前，我们以网上预售与专题宣传相结合的方式进行宣传，开始进行产品预热。我们提供的样章试读等服务引起了众多读者的关注，其结果是图书还没上市就有订单了（图书出版前的网上征订内容如右图所示）。



《网管员必读》系列图书出版前的征订

每本图书上市前我们都会设计专题的宣传资料，发布在专业网站、行业网站及实体书店等，最大范围地告知读者本套丛书的出版情况。此外，我们还抓住几次销售旺季，整合外部资源。比如，与《网管员世界》杂志合作，凡是购买这套图书的读者都可以获得一本《网管员世界》杂志；选择网上书店和实体书店同步开展这种互动式促销活动，形成书刊互动的营销模式……

正是在项目团队的努力下，《网管员必读》系列丛书在同类图书中脱颖而出，始终居于同类型图书的销售排行榜首位。时至今日，在我们回顾“网管员必读”系列丛书的成功与不足时，我们还是要特别感谢支持与鼓励我们的读者，正是有了广大读者的关爱与理解，才有了《网管员必读》系列丛书今日的成功。

《网管员必读》系列图书上市至今已有两年多了，在网络技术飞速发展的今天，作为出版者，我们有责任、有义务把最新最好的技术及时传送给广大读者。为此，我们与作者深入探讨，推出了《网管员必读》系列丛书第2版。新版图书不是“新瓶装旧酒”，换个封面，换点儿内容，而是彻头彻尾的大变革——技术内容进行了更新，应用案例进行了更换，体系结构也进行了调整。

希望《网管员必读》（第2版）能够继续成为院校和职场上的您的好帮手。

《网管员必读》项目组
2007年2月

X

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

内 容 简 介

本书虽然是《网管员必读——网络应用》的改版，但它绝不是简单的修改，而是完完全全的重写，内容更实用、更专业。全书共9章，13个大小方案，除了第1章的动态域名解析和端口映射配置属于公共应用以外，其他各章均介绍了适用于不同企业规模或者不同应用领域的多个应用方案，其中包括：Web 网站方案（分IIS 6.0和Apache 2.2两种）、FTP 站点方案（分IIS 6.0和Serv-U 6.3两种）、E-mail 服务器（分适用于中小型企业的POP 3、CMail 5.4.1两种方案，以及适用于大型企业的Exchange Server 2003方案）、RTX 2006企业即时通信方案、Windows Media Services 9.0流媒体服务器方案和SharePoint 企业门户网站方案。

相对于第1版来说，本书所介绍的应用案例更侧重于大中型企业的应用，如IIS 6.0和Apache 2.2的企业网站方案、Serv-U FTP 站点方案、Exchange Server 2003邮件服务器方案、Windows Media Services 9.0流媒体服务器方案和SharePoint 企业门户网站方案。其实这也是当前网络应用的一个主流发展趋势，因为现在绝大多数企业在经过了这么多年的发展以后，无论从其网络规模还是应用水平来说，较前几年有了很大的进步。

本书可以作为各类大专院校、网络应用培训机构的教材使用。本书还配备自学、教学课件，供大家免费下载，下载地址为：www.fecit.com.cn的“下载专区”。

未经许可，不得以任何方式复制或抄袭本书的部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网管员必读. 网络应用 / 王达编著. —2版. —北京：电子工业出版社，2007.2
ISBN 978-7-121-03793-1

I. 网… II. 王… III. 计算机网络—基本知识 IV. TP393

中国版本图书馆CIP数据核字（2007）第006711号

责任编辑：王树伟

印 刷：北京智力达印刷有限公司

装 订：北京中新伟业印刷有限公司

出版发行：电子工业出版社

北京海淀区万寿路173信箱 邮编：100036

开 本：787×1092 1/16 印张：40.25 字数：1030.4千字

印 次：2007年2月第1次印刷

印 数：6000册 定价：59.80元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。

质量投诉请发邮件至 zlt@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

溜客安全信息网

www.176ku.com

所提供书籍只限于技术参考时使用

请选择到官方论坛购买期刊支持正版书籍

本电子书严禁在淘宝开店出售，

禁止当做VIP收费项目等

尽量在本站下载安全的电子书刊

溜客精神：

技术共享，资源共享，资料共享

不求最好，只求较好

做中国较好的网络安全资料站

及时访问溜客安全网

第一时间下载技术资料

请将本站推荐给更多的好友

让大家都能成为溜客一员

溜客资料共享群：

访问溜客安全网最下方
查看本站最新共享QQ群

加入溜客资料共享群超大共享FTP等你来用

请勿重复加入群，给他人一点加入的空间

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

FOREWORD

目 录

第 1 章 动态域名解析与端口映射	1	2.2.1 IIS 6.0 的主要更改	28
1.1 动态域名解析	2	2.2.2 IIS 6.0 提供的服务	29
1.1.1 域名解析原理	2	2.2.3 IIS 6.0 的核心组件	30
1.1.2 动态域名解析概述	5	2.2.4 安装 IIS 及相关组件	31
1.1.3 配置动态域名解析 方案的基本步骤	6	2.3 组建新网站	38
1.2 动态域名解析服务的 申请与注册	6	2.4 网站基本配置	42
1.2.1 网域科技动态 域名解析	7	2.4.1 网站基本信息配置	42
1.2.2 每步数码公司的 动态域名解析	12	2.4.2 为网站指定主目录和 主页文件	45
1.3 端口映射	17	2.5 网站安全及配置	49
1.3.1 宽带路由器上的 端口映射	17	2.5.1 IIS 6.0 的主要 安全措施	49
1.3.2 ADSL MODEM 上的 端口映射	20	2.5.2 IIS 6.0 的应用程序 隔离模式	52
1.3.3 代理服务器上的 端口映射	21	2.5.3 隔离模式配置	55
第 2 章 IIS 6.0 Web 网站配置与管理	25	2.5.4 工作进程隔离模式中的 Web 应用程序隔离	58
2.1 利用 IIS 6.0 组建网站的 基本思路	26	2.5.5 IIS 5.0 隔离模式中的 Web 应用程序隔离 及配置	65
2.2 安装并启用 IIS 及相关组件	28	2.5.6 匿名身份验证及 配置	67
		2.5.7 基本身份验证及 配置	70

2.5.8 摘要式身份验证及配置.....	72	3.2.6 Apache 服务器配置基本思路.....	161
2.5.9 高级摘要式身份验证及配置.....	76	3.3 Apache 服务器程序的安装与调试.....	162
2.5.10 集成 Windows 身份验证及配置.....	77	3.4 Apache 服务器的全局配置.....	169
2.5.11 证书身份验证.....	78	3.4.1 服务器标识配置.....	169
2.5.12 .NET Passport 身份验证.....	80	3.4.2 文件定位配置.....	171
2.5.13 UNC 身份验证.....	82	3.4.3 资源使用限制配置.....	173
2.5.14 访问控制.....	82	3.4.4 其他全局配置.....	176
2.5.15 NTFS 权限.....	83	第 4 章 FTP 站点的配置与管理.....	181
2.5.16 TCP/IP 端口筛选.....	84	4.1 利用 IIS 6.0 创建 FTP 站点的基本思路.....	182
2.5.17 加密.....	88	4.2 安装 FTP 服务组件.....	182
2.6 虚拟目录创建与配置.....	92	4.3 新建 FTP 站点.....	183
2.6.1 虚拟目录的创建.....	93	4.3.1 FTP 站点的隔离模式.....	184
2.6.2 虚拟目录的配置.....	97	4.3.2 无隔离用户的 FTP 站点创建.....	186
2.6.3 虚拟目录的删除.....	98	4.3.3 IIS 管理器隔离用户 FTP 站点创建与配置.....	188
2.7 网站管理.....	98	4.3.4 Active Directory 隔离用户 FTP 站点的创建.....	189
2.7.1 IIS 网站管理基础.....	99	4.3.5 使用命令行脚本 iisftp.vbs 创建 FTP 站点.....	192
2.7.2 网站性能管理.....	101	4.4 FTP 站点基本配置.....	194
2.7.3 网站服务质量管理.....	106	4.5 FTP 站点安全配置.....	199
2.7.4 网站的其他管理.....	113	4.6 创建和配置 FTP 站点虚拟目录.....	204
2.7.5 网站的远程管理.....	119	4.6.1 FTP 虚拟目录概述.....	204
第 3 章 Apache 2.2 Web 网站配置.....	125	4.6.2 创建和删除 FTP 站点虚拟目录.....	205
3.1 Apache 2.2 基础.....	126	4.6.3 虚拟目录的配置.....	207
3.1.1 Apache 2.2 程序的组成.....	126	4.7 利用 Serv-U 组建 FTP 站点的基本思路.....	209
3.1.2 Apache 2.2 的新特性.....	128		
3.2 Apache 服务器配置文件.....	130		
3.2.1 Apache 配置文件基础.....	130		
3.2.2 配置段和容器.....	132		
3.2.3 Apache 2.2 的模块说明.....	137		
3.2.4 指令术语.....	139		
3.2.5 Apache 2.2 核心指令.....	142		

4.8	Serv-U 的安装与 FTP		5.1.3	POP3 电子邮件	
	站点创建	210		系统的组件	256
4.8.1	Serv-U 的安装	210	5.1.4	POP3 服务身份验证	258
4.8.2	利用设置向导创建		5.1.5	邮件存储区	260
	第 1 个 FTP 站点	211	5.1.6	POP3 邮件系统建设	
4.8.3	利用新建向导创建			基本思路	260
	FTP 站点	216	5.2	安装邮件服务器	261
4.9	服务器与域全局设置	219	5.2.1	利用“配置你的	
4.9.1	Serv-U 服务器的			服务器向导”进行	
	全局设置	219		安装	261
4.9.2	Windows 账户系统的		5.2.2	利用“添加或删除	
	FTP 域设置	222		程序”工具安装邮件	
4.9.3	自创用户系统的 FTP			服务器	266
	域站点设置	229	5.3	POP3 邮件服务器配置	267
4.10	自创用户系统的 FTP		5.3.1	邮件服务器配置	
	域用户和组设置	229		参考建议	268
4.10.1	用户设置	229	5.3.2	POP3 服务器	
4.10.2	组设置	233		属性配置	268
4.11	虚拟目录、用户和组创建	235	5.3.3	SMTP 虚拟服务器	
4.11.1	虚拟目录创建	235		属性配置	270
4.11.2	用户账户创建	238	5.4	POP3 邮件系统的	
4.11.3	组账户的创建	239		高级配置	276
4.12	FTP 站点的访问与管理	240	5.4.1	非安全密码身份验证	
4.12.1	FTP 站点的终端			方式下的磁盘配额	
	客户访问	240		配置	277
4.12.2	FTP 站点的		5.4.2	使用安全密码身份	
	远程连接	242		验证方式下的磁盘	
4.12.3	CuteFTP 的站点			配额应用	278
	全局配置	248	5.4.3	邮件发送配置	279
4.12.4	利用 CuteFTP 进行		5.5	客户系统的配置	283
	文件上传和下载	251	5.5.1	客户端邮箱的创建	283
第 5 章	中小型企业邮局系统	253	5.5.2	POP3 系统邮件	
5.1	POP3 电子邮件系统概述	254		客户端配置	285
5.1.1	POP3 邮件系统的		5.6	CMailServer 的企业邮局	
	两个基本协议	254		配置方案	288
5.1.2	电子邮件检索与		5.6.1	CMailServer 5.4.1	
	传输流程	255		简介	288

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.6.2 CMailServer 邮件 服务器系统的基本 配置思路.....	289	6.2.1 Exchange Server 2003 安装程序的改进	318
5.7 局域网邮件服务器的 建立与配置	291	6.2.2 Exchange Server 2003 安装前的准备	320
5.7.1 局域网内部邮件 服务器的基本配置	291	6.2.3 服务器安装前的 系统准备	322
5.7.2 邮箱账号创建与配置 ..	295	6.2.4 程序安装前的 7 个 准备步骤	324
5.7.3 用户组的建立	300	6.2.5 Exchange 程序的 正式安装	332
5.7.4 客户端 Outlook Express 的配置	301	6.2.6 Exchange Server 2003 的无人值守安装	334
5.8 其他类型邮件服务器建立 与配置	302	6.3 Exchange Server 2003 服务器配置	337
5.8.1 互联网邮件服务器 建立与配置	302	6.3.1 Exchange Server 2003 服务器根节点 属性配置	337
5.8.2 局域网拨号邮件 服务器	303	6.3.2 “全局设置”节点 属性配置	339
5.8.3 多域名邮件服务器 建立与配置	304	6.4 邮件服务器属性设置	349
5.9 CMailServer 邮件服务器的 维护与管理	305	6.5 公用文件夹存储和邮箱 存储的创建与设置	361
5.9.1 CMailServer 企业 邮局的维护	305	6.5.1 公用文件夹层次 结构创建	362
5.9.2 CMailServer 邮件 服务器的基本管理	308	6.5.2 配置新的公用 文件夹	365
第 6 章 大中型企业邮局系统	311	6.5.3 允许公用文件夹 接收邮件	368
6.1 Exchange Server 2003 简介 ..	312	6.5.4 公用文件夹 存储设置	372
6.1.1 Exchange Server 2003 的两个版本	312	6.5.5 邮箱存储创建与 配置	374
6.1.2 Exchange Server 2003 支持的环境	313	6.6 用户、组邮箱创建与配置 ..	377
6.1.3 Exchange Server 2003 技术概述	313	6.6.1 已启用邮箱和已启用邮 件的收件人的配置	377
6.1.4 Exchange Server 2003 邮件服务器系统的 基本部署思路	316	6.6.2 使现有的 Active Directory 用户对象 成为收件人	382
6.2 Exchange Server 2003 的 部署与安装	318	6.6.3 为组对象启用邮件	385

6.7 策略的创建与管理..... 387	6.11.4 使用队列查看器 管理邮件.....429
6.7.1 创建服务器策略..... 387	6.11.5 配置 SMTP 的诊断 日志记录.....433
6.7.2 创建公用存储策略..... 388	
6.7.3 创建邮箱存储策略..... 390	
6.7.4 创建收件人策略..... 392	
6.7.5 将系统策略 应用于对象..... 396	
6.8 SMTP 协议配置..... 397	第 7 章 企业即时通信系统.....435
6.8.1 使用向导配置 Internet 邮件..... 397	7.1 即时通信基础.....436
6.8.2 使用向导配置双 宿主服务器..... 401	7.1.1 腾讯 RTX 简介.....436
6.8.3 手动配置 Internet 邮件的发送..... 402	7.1.2 RTX2006 的 主要特性.....437
6.8.4 手动配置 Internet 邮件的接收..... 404	7.1.3 RTX 2006 的 安全技术.....439
6.9 地址列表..... 407	7.1.4 RTX2006 系统的 基本部署思路.....440
6.9.1 地址列表概述..... 407	7.2 RTX 管理器的设置.....443
6.9.2 创建地址列表..... 407	7.3 部署组织架构.....446
6.9.3 创建地址列表..... 408	7.3.1 添加一级部门.....446
6.10 Exchange 客户端的设置..... 410	7.3.2 添加多级部门.....448
6.10.1 Outlook 2003 的 客户端配置..... 410	7.3.3 新建组织架构.....449
6.10.2 准备管理客户端 访问..... 413	7.4 管理用户信息.....450
6.10.3 配置 Outlook 2003 缓存 Exchange 模式..... 414	7.4.1 添加单个用户.....451
6.10.4 使用 Outlook Web Access 访问..... 416	7.4.2 批量导入用户数据.....453
6.10.5 在 Outlook 中创建 公用文件夹..... 419	7.4.3 为用户分配权限.....454
6.11 邮件服务器管理..... 421	7.5 客户端设置与使用.....459
6.11.1 管理收件人权限..... 421	7.5.1 个人设定.....460
6.11.2 Exchange 管理委派 向导..... 425	7.5.2 系统设置.....462
6.11.3 管理邮箱存储和 公用文件夹存储..... 426	7.5.3 添加联系人.....464
	7.5.4 多功能会话.....466
	第 8 章 企业流媒体服务器系统.....471
	8.1 流媒体基础.....472
	8.1.1 下载内容与 流式播放.....472
	8.1.2 流式媒体系统概述.....473
	8.1.3 了解 Windows Media 9 系列.....474
	8.1.4 与流式媒体播放 有关的术语.....476

8.1.5 配置 Windows Media 9 流媒体服务器系统的 基本思路.....	478	8.6 内容管理与制作	525
8.2 流媒体服务器安装.....	479	8.6.1 预先录制的 内容概述.....	526
8.2.1 Windows Media 服务的安装.....	480	8.6.2 创建播放列表.....	528
8.2.2 Windows Media 编码器的安装.....	484	8.6.3 使用 Windows Media 播放列表编辑器创建 包装播放列表	532
8.3 Windows Media Services 服务器配置	485	8.6.4 广告方案概述.....	534
8.3.1 “授权”插件 属性配置.....	485	8.6.5 在流中添加 包装广告	535
8.3.2 “日志记录”插件 属性配置.....	489	8.7 Windows Media 编码器的 使用	536
8.3.3 “事件通知”插件 属性配置.....	491	8.7.1 广播实况事件.....	537
8.3.4 “验证”插件 属性配置.....	494	8.7.2 捕获音频或视频.....	539
8.3.5 “控制协议”插件 属性配置.....	497	8.7.3 转换文件.....	540
8.3.6 “限制”插件 属性配置.....	504	8.7.4 捕获屏幕.....	541
8.4 部署 Windows Media Services 服务器	505	第 9 章 企业 SharePoint 门户 网站配置.....	543
8.4.1 Windows Media Services 服务器部署概述.....	506	9.1 Windows SharePoint Services 和 SharePoint Portal Server.....	544
8.4.2 部署过程中需要 考虑的问题.....	507	9.1.1 Windows SharePoint Services 2.0.....	544
8.4.3 容量计划	510	9.1.2 SharePoint Portal Server 2003.....	546
8.4.4 执行负载平衡和 群集化.....	512	9.1.3 SharePoint Portal Server 与 SharePoint Services 之间的关系	550
8.4.5 了解可扩展性	514	9.1.4 配置 SharePoint 门户 网站的基本思路	551
8.4.6 了解容错	515	9.2 程序安装及其注意事项	552
8.4.7 监视服务器性能	516	9.2.1 程序安装条件.....	553
8.5 发布媒体内容.....	518	9.2.2 SharePoint Services 程序的安装	554
8.5.1 添加发布点	519	9.2.3 SharePoint Portal Server 2003 服务器的安装	558
8.5.2 配置发布点	521	9.3 SharePoint Services 虚拟 服务器配置	563
8.5.3 从发布点进行 流式播放.....	524		

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.3.1	SharePoint Services 站点基础.....	563
9.3.2	网站用户和权限	564
9.3.3	SharePoint Services 虚拟服务器扩展.....	566
9.3.4	扩展后的虚拟 服务器配置.....	568
9.3.5	SharePoint 网站 集安全配置.....	574
9.4	SharePoint 网站的 配置与使用	577
9.4.1	网站模板的选择	577
9.4.2	SharePoint 网站文档库 配置与使用.....	579
9.4.3	SharePoint 网站图片库 配置与使用.....	587
9.4.4	SharePoint 网站列表 配置与使用.....	588
9.4.5	讨论板的配置 与使用.....	593
9.4.6	调查项目的配置与 使用.....	596
9.5	SharePoint Portal Server 2003 服务器的配置	598
9.5.1	SharePoint Portal Server 服务器配置	598
9.5.2	创建门户网站.....	601
9.5.3	门户网站的配置.....	602
9.5.4	配置门户网站安全性.....	607
9.5.5	为门户网站添加 SharePoint 站点.....	610
9.5.6	为门户网站添加 个人网站	614
9.6	SharePoint Portal Server 2003 企业门户网站的管理	618
9.6.1	SharePoint Services 服务器管理概述	618
9.6.2	SharePoint Portal Server 企业门户网站的 基本管理	620
9.6.3	门户网站的 作业管理	623



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

**你
想
换
吗
？**

www.17huan.com

第 1 章 动态域名解析与端口映射

以前个人用户要架设自己的个人网站（其实只是个人主页）通常是挂靠在一些 NSP（网络服务商）网站上，这样一来只能拥有二级以下域名，因为那时互联网上的服务器都必须有固定的互联网 IP 地址。对于普通个人用户来说，域名还好说，到处可以申请到，可是固定的互联网 IP 地址就不好得到，因为公网 IP 地址非常匮乏，不可能做到想申请就有，特别是针对个人用户。当然，那时互联网接入技术也不先进，最多也只能是 128Kbps（对于普通个人用户而言）的 ISDN（其实当时个人用户普遍还是 56Kbps 的 MODEM 拨号接入），要使自己的服务器承受起大量的用户访问谈何容易。

可是，随着宽带接入技术和动态域名解析服务（DDNS）的普及应用，现在要架设自己的互联网服务器已经非常容易了，因为以上两大难题均已全面解决。只要自己制作好网站，向提供动态域名解析服务的 NSP 申请一个域名，再加上一条现在普及的宽带互联网接入线路（不要求是固定 IP 的专线接入，如 PPPoE ADSL、动态 FTTx 和 Cable MODEM），就可以大功告成了，无须申请固定的互联网 IP 地址。正是这一原因，现在绝大多数企业都架设了自己的互联网 Web 服务器、FTP 服务器、邮件服务器等，对自己企业进行全面信息化武装。个人网站更是全面取代了以前挂靠式的个人主页，而且个人用户都可以轻松拥有与跨国公司一样的一级域名网站，只是个人用户通常采用 DDNS 而已。

本章要向大家介绍 DDNS 的申请和配置方法，因为本书后面将要介绍的动态 Web 服务器、FTP 服务器和邮件服务器等都需要用到。

本章重点

- 域名和动态域名解析原理
- 花生壳域名解析服务的申请与使用
- 每步动态域名解析服务的申请与使用
- 宽带路由器、ADSL MODEM 端口映射
- 端口镜像软件 portTunnel 的端口镜像配置

1.1 动态域名解析

目前在网站的域名解析中，除了可以使用静态 IP 地址+域名方案外，还有一种被称为“动态域名解析服务”（DDNS）的方案，它是采用动态 IP 地址+域名的方案。这就使得没有合法静态互联网地址的用户都可以通过所申请到的域名把自己的各种服务器放在互联网上供全球互联网用户访问、使用。这就是本章要介绍的主题。不过，在正式介绍“动态域名解析服务”（DDNS）之前，首先来简单了解一下“域名解析服务”（DNS），因为 DDNS 是 DNS 中的一种。

1.1.1 域名解析原理

在互联网上，最终确定访问主机位置的不是域名，也不是计算机的 MAC 地址，而是 IP 地址。而 DNS 服务，或者叫域名服务、域名解析服务，就是提供域名与 IP 地址的相互转换，也可以说是一种对应（映射）关联。在 DNS 服务器中通常会有一个域名与 IP 地址的映射表，以便用户无论是输入服务器名（相当于域名），还是服务器的 IP 地址都可以及时得到转换，查找到相应的服务器。这就是在局域网中，通常要把局域网中的邮件服务器域名记录也添加到 DNS 记录的原因了。

IP 地址（特指 IPv4 地址）是由一个共 12 位的分段数字组成的，中间用句点将其分隔为 4 部分（例如，192.161.1.42）。之所以有了 IP 地址，还要域名，那是因为数字格式的 IP 地址难以记忆，而域名一般都有代表性（如公司名称），便于记忆，如 www.grfwgz.com 等。其实这也方便了所使用的域名实现个性化更改，但 IP 地址可以总是不变的。如果用户在浏览器地址栏中输入的是域名，则必须转换成对应的 IP 地址，这就是域名解析过程。



无论网站采用的是静态 IP 地址+域名方案（DNS 方案），还是动态 IP 地址+域名方案（DDNS 方案），要成功访问相应互联网服务器，就必须准确地知道相应服务器当前的互联网 IP 地址。并不是像许多网友所认为的，DDNS 方案中无须知道确切的服务器 IP 地址。只是这个 IP 地址是动态变化的，每次访问，服务器的 IP 地址可能都不一样。这就需要提供 DDNS 的软件系统来把服务器当前的 IP 地址及时告诉相应的服务器域名。

域名解析有正向解析和反向解析之说，正向解析就是将域名转换成对应的 IP 地址的过程，它应用于在浏览器地址栏中输入网站域名时的情形；而反向解析是将 IP 地址转换成对应域名的过程，但在访问网站时无须进行反向解析，即使在浏览器地址栏中输入的是网站服务器 IP 地址，因为互联网主机的定位本身就是通过 IP 地址进行的，只是在同一 IP 地址下映射多个域名时需要。另外反向解析经常被一些后台程序使用，用户看不到。

除了正向、反向解析之外，还有一种称为“递归查询”的解析。“递归查询”的基本含义就是在某个 DNS 服务器上查找不到相应的域名与 IP 地址对应关系时，自动转到另外一台 DNS 服务器上查询。通常递归到的另一台 DNS 服务器对应域的根 DNS 服务器。因为对于提供互联网域名解析的互联网服务商，无论从性能上，还是从安全上来说，都不可能只有

一台 DNS 服务器，而是由一台或者两台根 DNS 服务器（两台根 DNS 服务器通常是镜像关系），然后再在下面配置了多台子 DNS 服务器来均衡负载的（各子 DNS 服务器都是从根 DNS 服务器中复制查询信息的），根 DNS 服务器一般不接受用户的直接查询，只接受子 DNS 服务器的递归查询，以确保整个域名服务器系统的可用性。当用户访问某网站时，在输入了网站网址（其实就包括了域名）后，首先就有一台首选子 DNS 服务器进行解析，如果在它的域名和 IP 地址映射表中查询到相应的网站的 IP 地址，则立即可以访问，如果在当前子 DNS 服务器上没有查找到相应域名所对应的 IP 地址，它就会自动把查询请求转到根 DNS 服务器上进行查询。如果是相应域名服务商的域名，在根 DNS 服务器中是肯定可以查询到相应域名 IP 地址的，如果访问的不是相应域名服务商域名下的网站，则会把相应查询转到对应域名服务商的域名服务器上。

现在假设要访问 example.microsoft.com 网站，整个递归查询过程如图 1-1 所示。具体步骤序列号和响应方向均已在图中标注。递归查询部分体现在（4）、（6）和（8）这 3 步。具体说明如下。

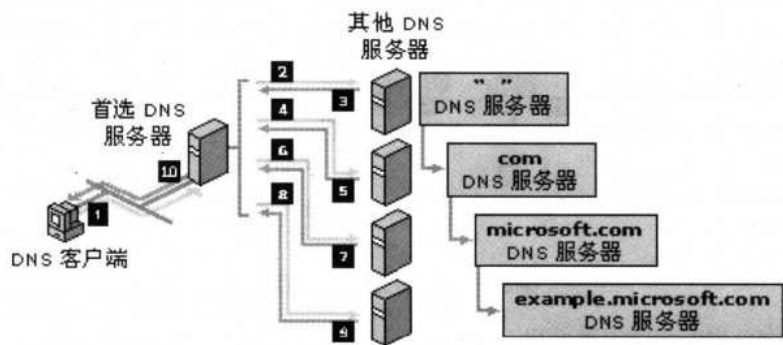


图 1-1 递归过程示例

客户端发起访问后，首先由首选服务器分析全名，并确定顶级域“com”具有权威性控制的服务器的位置，于是通过图中的第（4）步递归到“com”DNS 服务器，以便获取“.com”服务器的参考信息。这一步包括了图中的第（1）~（4）四步。

然后进一步分析，发现所访问的网址需要对一级域名 microsoft.com 域名位置进行确定，发送反馈信息，再通过图中的第（6）步继续使用递归查询递归到“microsoft.com”DNS 服务器上，以便获取“microsoft.com”服务器的参考信息。本步骤包括图中的第（5）和第（6）两步。

再进一步分析又得到，所查询的服务器域名还包括二级域名“example”，继续反馈信息，来自“microsoft.com”服务器的参考性应答再通过图中的第（8）步递归到“example.microsoft.com”DNS 服务器，以便获取“example.microsoft.com”服务器的参考信息。本步骤包括图中的第（8）和第（9）两步。

最后，与服务器“example.microsoft.com”联系上并解析后，因为再没有下级的域名了，所以它向启动递归的源服务器作出权威性地应答。当源服务器接收到表明已获得对请求查询的权威性应答的响应时，它将此应答转发给发出请求的客户端。本步骤包括图中的第（9）

4 网管员必读——网络应用（第2版）

和第（10）两步。
通过以上 10 个步骤后，就完成了整个递归查询过程。

尽管执行上述递归查询过程可能需要占用大量资源，但对于 DNS 服务器来说它仍然具有一些性能上的优势。例如，在递归过程中，执行递归查询的 DNS 服务器，获得有关 DNS 域名空间的信息。该信息由服务器缓存起来并可再次使用，以便提高使用此信息或与之匹配的后续查询的应答速度。虽然打开与关闭 DNS 服务时，这些缓存信息将被清除，但是随着时间的推移，它们会不断增加并占据大量的服务器内存资源。

其实以上递归查询，在局域网中有相应的应用，如图 1-2 所示就是一个包括递归查询的完整名称解析过程图。其中的 Q1，Q2，Q3…代表询问的序号号；而 A1，A2，A3…则代表对应上述询问序号号的应答序号号。

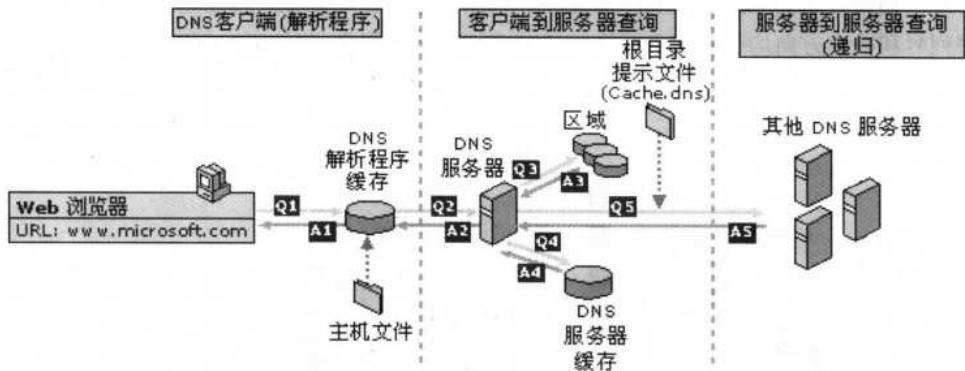


图 1-2 完整的 DNS 查询过程

通过查询过程的初始步骤可知，DNS 域名由本机的程序使用。该请求随后传送至 DNS 客户服务，以便使用本地缓存信息进行解析。如果可以解析查询的名称，则应答该查询，处理完成。当然要真正实施递归查询，必须在本地网络系统中配置多台 DNS 服务器，并且配置递归查询选项设置，如图 1-3 所示的对话框是在配置 DNS 服务器时打开的，在这里可以递归查询到服务器的地址；而如图 1-4 所示则是要在 DNS 服务器属性设置中禁用递归查询功能。

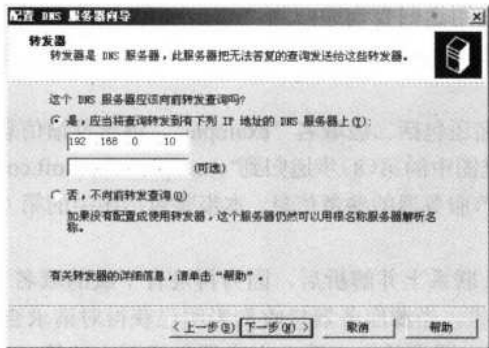


图 1-3 递归查询服务器配置对话框



图 1-4 DNS 服务器属性对话框“高级”选项卡

1.1.2 动态域名解析概述

如果你的计算机想参与互联网通信，无论是作为一台执行资源访问的客户端，还是作为一台被访问的资源提供服务器，你的计算机都必须有一个合法的 IP 地址（如 61.10.15.188），这个地址通常由互联网服务商（SP）提供给你。这种 IP 地址的分配又有静态和动态两种，通常作为服务器的计算机的 IP 地址是静态的（固定），因为它要为用户提供服务，为什么呢？试想，如果一台服务器的 IP 地址每天变换，那又有哪个用户可以记住服务器的地址呢？而作为访问客户端的计算机绝大多数时间是作为资源请求方，而不是服务提供者，因此它的 IP 可以是动态的。通常体现在每次拨号得到的 IP 地址都不同，当用户断线时再由服务商回收再分配。

可不可以让所有的计算机的 IP 地址都固定呢，不管是服务器还是客户端，那样不就可以互相访问了吗？事实上，目前的 IP 地址已经非常匮乏，一个固定 IP 地址的租用费用是十分昂贵的（各地电信服务商的价格不同，一般是按使用年限计费，从几千元到几万元不等）；而且由于互联网 IP 地址非常有限。

为了解决这一难题，早在两年前开始就有服务商开发出了一种能动态解析域名 IP 地址的 DNS 服务，那就是动态域名解析服务（DDNS）。有了它，用户就无须有固定的互联网 IP 地址了，只需有一个域名，再加上一条任意接入方式的互联网线路就可以部署互联网服务器了。

动态 DNS（域名解析）服务，就可以将固定的互联网域名和动态（非固定）IP 地址实时对应（解析）起来，其实它的作用就是及时把当前互联网服务器的 IP 地址告诉对应的 DNS 服务商，把相应的域名与动态 IP 地址中当前所分配到的 IP 地址对应起来。用户每次上网得到新的 IP 地址之后，安装在用户计算机里的动态域名软件就会把这个 IP 地址发送到动态域名解析服务器，更新域名解析数据库。Internet 上的其他人要访问这个域名的时候，动态域名解析服务器会返回正确的 IP 地址给他。也就是说，尽管是动态域名解析方案，最终还是把域名解析成对应服务器上所分配到的互联网 IP 地址上，只不过这个 IP 地址不是固定的而已。

相对于传统的静态 DNS 而言，DDNS 可以将一个固定的域名解析到一个动态的 IP 地址。简单地说，不管用户何时上网、以何种方式上网、得到一个什么样的 IP 地址、IP 地址是否会变化，都能保证通过一个固定的域名就能访问到用户的计算机。这就意味着在动态 DNS 服务下的计算机就好像具有了固定的 IP 地址，可以充当互联网服务器了。对于广大互联网用户和中小企业而言这无疑是一项非常具有吸引力的服务。

不难看出，利用动态 DNS 构建服务器具有费用低廉（无须申请昂贵的固定 IP 地址）、功能全面、实施灵活的多种优势。同时，利用动态 DNS 构建服务器也可以和其他的现有服务，例如虚拟主机服务，相配套组成更灵活的服务。因为绝大部分 Internet 用户上网的时候分配到的 IP 地址都是动态的，用传统的静态域名解析方法，用户想把自己上网的计算机做成一个有固定域名的网站是不可能的。而有了动态域名，这个美梦就可以成真。用户可以申请一个域名，利用动态域名解析服务，把域名与自己上网的计算机绑定在一起，这样就可以在家里或公司里搭建自己的网站，非常方便。

对于使用动态 IP 接入的用户而言，包括普通电话线、ISDN、ADSL、有线电视网络、双绞线到户的宽带网和其他任何能够提供互联网真实 IP 的接入服务线路，要架设自己独立的服务器必须借助动态域名解析服务。动态域名解析服务有收费的和免费的两种，如 88IP（收费）、

6 网管员必读——网络应用（第2版）

DNS2GO（收费）、“花生壳”和每步动态域名解析（均有免费和收费两种）。网上还有很多这类软件。

1.1.3 配置动态域名解析方案的基本步骤

在静态域名解析中，要使用户可以访问 Intranet 或 Internet 上的站点，必须使得相应网站的域名与对应的静态 IP 地址对应，以便 DNS 服务对所访问的网站进行正向、反向解析。这样，无论用户在浏览器地址栏中输入的是网站域名，还是相应网站所分配的静态 IP 地址，都可以访问到网站。但因为域名和 IP 地址都是静态的，所以也就无须申请特别的域名解析服务，如果是互联网服务器，则只需申请域名和固定的互联网 IP 地址即可；如果是用于局域网的服务器，则只需自己配置局域网内部的 DNS 服务器（具体配置方法参见本系列丛书的《网管员必读——网络组建》一书），并给服务器分配一个静态的 IP 地址即可。

动态域名解析方案中，域名的申请与静态域名解析方案是一样的。而不同的互联网线路的配置又有些区别，因为静态域名解析方案中需要静态的互联网 IP 地址，所以通常采用的是专线互联网接入，如专线 ADSL、专线 Cable MODEM 和租用 ISP 专线等。除此之外，还需要向提供 DDNS 的 ISP 申请动态域名解析服务，在自己的服务器上安装对应的动态域名解析客户端软件。以下是动态域名解析方案配置的基本步骤。

（1）在一家提供动态域名解析服务的网站注册动态解析用户，如 www.88IP.com（88IP 宽带 e 联）、www.Meibu.com（每步科技）、www.vavic.com（网域科技）。

（2）用 IIS、Apache 等其他网站软件组建自己的 Web 网站、FTP 站点或者邮件服务器。并把上一步所申请到的域名配置在网站和邮件服务器中。至于 FTP 站点，有些 FTP 服务器软件组建的 FTP 站点也需要配置域名，如 Serv-u，而 IIS 中的 FTP 站点无须配置域名。具体在本书后面各章有介绍。

（3）制作自己网站上的网页文件，当然也可以在已有网站上下载网站源码，然后经过适当的编辑，变成自己的网站。再把这些网站文件放到这些 Web 网站、FTP 站点主目录中，邮件服务器中无须添加这些文件。

（4）利用任意动态互联网接入方式（通常动态域名解析方案中采用的是动态接入方式，如果采用专线方式，再用动态域名解析方案就失去了意义）连接到互联网，下载相应服务商提供的动态解析客户端软件，并用注册的用户登录。

（5）如果外网是直接连接到代理服务器上的，则下载端口映射软件，把该软件安装在代理服务器上，进行端口映射软件设置；如果外网直接连接到路由器，则提供路由功能的 ADSL。

1.2 动态域名解析服务的申请与注册

“动态域名”因宽带而生，同时也大大拓宽了基于宽带的网络应用空间。随着宽带网络的飞跃发展，越来越多的中小企业和玩家开始使用这种能够对动态 IP 进行解析和正确寻址的服务，建立自己的网络应用。同时，众多厂商也开始盯上了这块巨大的面包。

一般来说，一个动态域名解析系统由两部分组成：一部分是服务器端程序，通常位于 ISP 的 DNS 服务器上，由它负责提供 DNS 服务以及实现实时动态域名解析；另一部分是客户端程序，安装在采用动态域名解析方案的互联网服务器上。客户端程序负责在用户每次上网时把本机的 IP 地址告诉服务器端程序，在收到客户端通知后服务器端程序可立即更新原域名的解析映射，将新的 IP 地址重新与原有的固定域名相对应，这样就实现了动态 IP 到域名的同步映射。通过使用动态域名解析系统，你的网站即使没有静态 IP 地址，互联网上的访问者也能通过输入固定域名来拜访你的个人家园。

尽管各种动态域名解析系统在运行使用和功能特色上有差别，但其工作原理都是一样的，且安装配置的流程也基本一致，一般都要经过以下 3 个步骤：（1）申请账号，并注册域名；（2）安装配置客户端；（3）联网并运行客户端软件。本节要介绍的是目前国内比较典型的两款动态域名解析软件，也是两大动态域名申请和解析服务商——广州网域科技公司的“花生壳”和青岛每步科技公司的每步动态域名解析服务申请和使用方法。

1.2.1 网域科技动态域名解析

“花生壳”是广州网域科技公司开发的一款完全免费（收取的服务费主要体现在顶级域名申请上）的动态域名解析服务客户端软件。当你安装并注册该项服务，无论你在任何地点、任何时间、使用任何线路，均可利用这一服务建立拥有固定域名和最大自主权的互联网主机。

“花生壳”支持的线路包括普通电话线、ISDN、ADSL、Cable MODEM、FTTH 的宽带网和其他任何能够提供互联网真实 IP 的接入服务线路，而无论连接获得的 IP 属于动态还是静态。对于使用动态 IP 接入的用户而言，可以利用“花生壳”软件在办公室或家庭建立拥有固定域名的互联网主机。由于不受线路类型、主机存放地点的约束，所以可以根据自己的需求选择合适的系统平台、数据库平台和站点运营模式，并由此获得最大限度的自主性。

利用“花生壳”软件实现网站动态域名解析的配置步骤如下。

1. 申请“花生壳”护照

要利用“花生壳”域名动态解析软件，就得先在网域科技公司的网站上申请护照，也就是用户的账户。申请网域科技公司“花生壳”护照的步骤如下。

（1）在 IE 地址栏键入 <http://www.oray.net> 地址，打开如图 1-5 所示界面。



图 1-5 网域科技公司网站上的控制台窗口

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8 网管员必读——网络应用（第2版）

(2) 在界面中的“我的控制台”窗口中单击【免费注册】按钮开始申请“花生壳”护照，打开如图 1-6 所示界面。在这里要填写护照名，就相当于网站用户名。因为所申请的护照名可能其他人已经用了，所要输入后单击【检查护照是否可用】按钮看一下是否可用。然后输入保护护照的密码，以及密码提示问题和自己用来联系的电子邮件账户。

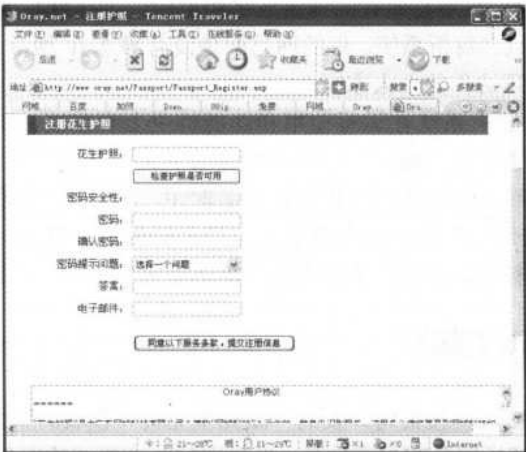


图 1-6 “注册花生壳热护照”界面

(3) 填写好以上信息后，看一下下面的用户协议，确认可以接受后，单击【同意以下服务条款，提交注册信息】按钮，返回到类似图 1-5 所示的登录控制台。在这里可以把上一步配置的护照信息在网站上登录了。成功后即可在“我的控制台”中见到自己的护照了，如图 1-7 所示。此时护照申请就成功了。



图 1-7 申请的护照在“我的控制台”中的显示

下一步就是申请域名了，如果已有域名，则不用申请，但需要做域名转入，这将在本章后面具体介绍。在这里先介绍在网域科技公司申请免费的二级域名的方法，这对于绝大多数个人用户来说是首要选择。

2. 申请免费域名

护照申请成功后还需要申请属于自己网站的域名。这里要说明一点，护照并不代表域名，也就是说，一个护照可以申请很多个域名。

(1) 在如图 1-7 所示界面左下角单击【申请免费域名】（也可以选择注册其他域名，只不过注册其他域名需要收费），打开如图 1-8 所示界面。首先要求用所申请的护照登录。



图 1-8 “登录到我的控制台”界面

(2) 登录成功后，在打开的界面中选择“免费域名”选项卡，进入如图 1-9 所示界面。在下面的文本框中直接输入想申请的域名的前部分，也称主机头部分，在后面的下拉列表中选择所想用的免费域名后缀。



图 1-9 申请免费域名界面

此时也要单击一下【查询】按钮看看目前所申请的域名是否可用，以免所申请的域名在该网站已被使用过，因为互联网上的域名必须唯一。查询的结果会在下面显示，把鼠标放在上面即可知道所申请的域名是否已注册，如果是未注册的才可以继续注册，如图 1-10 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10 网管员必读——网络应用（第2版）



图 1-10 域名查询结果显示



注意 在网域科技中，标准的免费用户只能申请 vicp.net、oicp.net、eicp.net、xicp.net、vicp.cc、5166.info 和 51vip.biz 后缀的免费域名。

(3) 单击显示未注册的域名，显示如图 1-11 所示界面。单击【确认申请】按钮，然后选择“是”单选项。

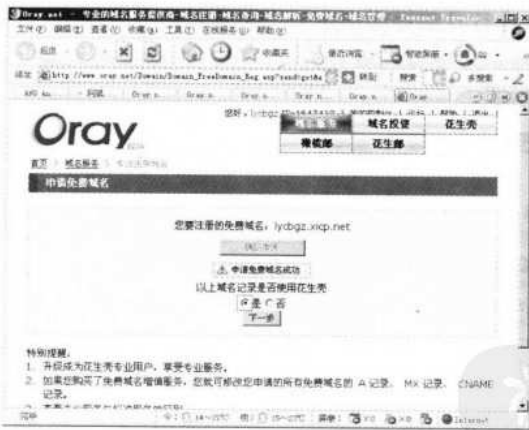



图 1-11 域名申请确认界面

(4) 单击【下一步】按钮，打开如图 1-12 所示界面。在其中选择网站类型和其他一些基本信息，如网站描述、网站更新提示、在线时间。并阅读下面的协议条款。

(5) 单击【同意以下服务条款，提交信息】按钮后，立即显示  激活花生壳服务成功！，此时表明所申请的域名已成功生效了。可以正式使用所申请的免费域名了。

接下来要做的就是从网站上下载花生壳客户端程序，用它来进行日常的网站登录（只有登录后才可使用花生壳的动态域名解析服务）和基本的网站管理。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

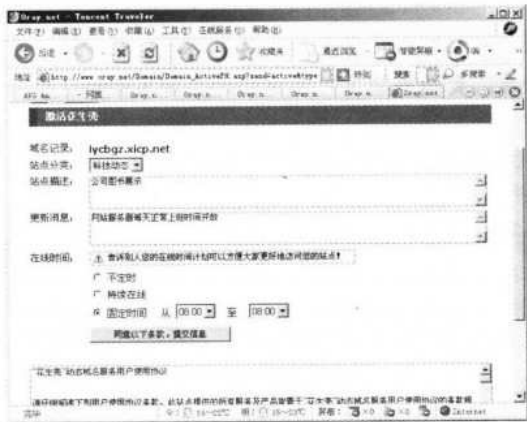


图 1-12 “激活花生壳”服务界面

花生壳客户端软件的下载可在 <http://dl.pconline.com.cn/html/1/3/dlid=6153&dltypeid=1&pn=0&.html> 网址中进行，目前最新版本为 3.9.1。

3. 客户端软件的使用

下载花生壳客户端程序后即可解压安装，安装完后运行它，打开如图 1-13 所示的用户登录控制台。在这里输入护照账号和密码（注意：这里输入的不是域名，而是护照名），输入好后单击【登录】按钮即可成功登录花生壳网站。

成功后界面的左下角看到一个小小的立方体，如果是红绿蓝三色，并在旁边显示“在线”字样，并在“免费域名”栏中显示已申请有域名，如图 1-14 所示，则说明域名解析成功。以后只要在网上，它就会自动帮助解析了。花生壳客户端软件一般会设置成服务，自动随系统的启动而启动。每次上网时，它会自动监视每次上网的 IP 地址，自动追踪并将其与所申请的网域名称相对应，并及时把相应的 IP 地址反馈到所在网域科技公司 DNS 服务器上，更新你所申请的免费域名配置信息。以后别人只要用固定的域名就可以连接上你架设的网页服务器，尽管上网时所分配的 IP 地址每次都不同，也不会受到影响。



图 1-13 花生壳客户端登录控制台



图 1-14 登录成功后的控制台



注意 要确保网站时刻能被用户成功访问到，就必须一直开启这一客户端软件，并成功登录。否则不能进行正确的动态域名解析。

4. 域名转入

对于不是在网域科技公司申请注册的域名，通过转入域名 DNS，一样可以享受网域科技公司提供的所有域名服务。转入域名 DNS 前，请联系注册商修改所申请的域名对应的域名记录 NS 为 ns1.oray.net 和 ns2.oray.net，IP 分别为 61.152.96.114 和 219.136.252.78。另外，为了保证服务的稳定性，请确保 NS 记录仅有 ns1.oray.net 和 ns2.oray.net，删除原来 ISP 的 NS。修改 NS（DNS）记录一般需 24~48 小时才能生效，使用前可先使用 DOS 命令 nslookup -q=ns yourdomain 202.96.128.166 查询，正确显示表示成功解析。转入域名 DNS 成功后，以后的域名续费还需要在原注册商进行续费。

域名转入的方法很简单，只需先按以上步骤请求域名原注册商配置 DNS 记录，然后在如图 1-9 所示界面左边导航栏中单击【转入域名 DNS】链接，打开如图 1-15 所示界面。

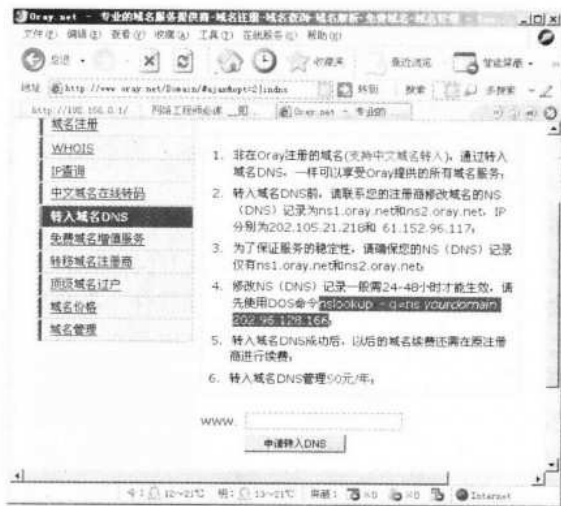


图 1-15 “转入域名 DNS” 界面

在域名注册商的 DNS 服务器上配置好后，在如图 1-15 所示界面底部输入要转入 DNS 域名，然后单击【申请转入 DNS】按钮即可（注意，这里转入的域名只能是以 WWW 开头的顶级域名）。

1.2.2 每步数码公司的动态域名解析

由每步数码推出的动态域名解析系统应该算是最容易使用的傻瓜级产品，它支持国际域名，也提供众多的免费二级域名供用户选择。目前每步提供了 3 个版本的客户端软件，分别支持单用户、多用户和具有固定 IP 地址的用户使用。客户端软件、二级域名申请及其动态域名解析均免费。

每步数码公司的动态域名解析服务申请步骤与前面介绍的网域科技公司的花生壳动态

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

域名解析服务申请有些不一样，它没有像“花生壳”那样分块进行，而是在一个注册向导中完成了域名和护照（在这里两者是一样的，就是域名）申请的全部步骤。

1. 域名申请和软件下载

(1) 登录到每步数码公司动态域名解析的网站主页：<http://www.meibu.com/index.asp>，如图 1-16 所示。



图 1-16 每步数码公司动态域名解析网站主页

(2) 在界面左上角的“用户登录”窗口中单击【免费注册】按钮，打开如图 1-17 所示注册信息输入界面。在这里所要填写的项目比较简单，带*号才需要填写，而且同时要输入你所申请的域名。不过，这里提供的免费二级域名后缀只有 meibu.com 这样一个，相比前面介绍的网域科技公司来说有较大局限性。

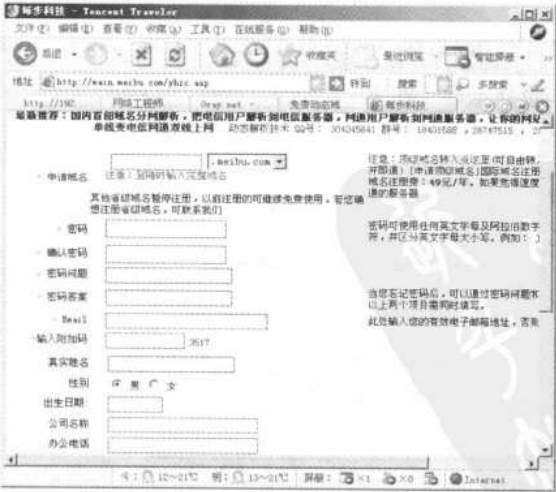


图 1-17 每步数码公司免费二级域名注册界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

14 网管员必读——网络应用（第2版）



在这里除了可以注册二级域名，还可以注册顶级域名，方法是单击界面右上部红色字体的【注意：顶级域名转入点这里】链接，此时打开的是另一个注册界面，如图 1-18 所示。在此仅以免费域名申请为例进行介绍。



图 1-18 每步数码公司收费项级域名注册界面

注册成功后会弹出如图 1-19 所示提示。

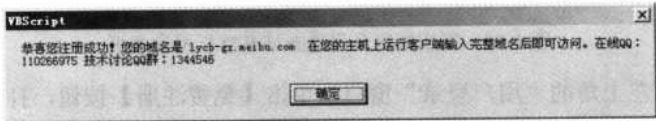


图 1-19 域名注册成功后的提示框

(3) 单击【确定】按钮后，转入客户端下载界面，如图 1-20 所示，可根据需要下载合适的客户端软件版本。

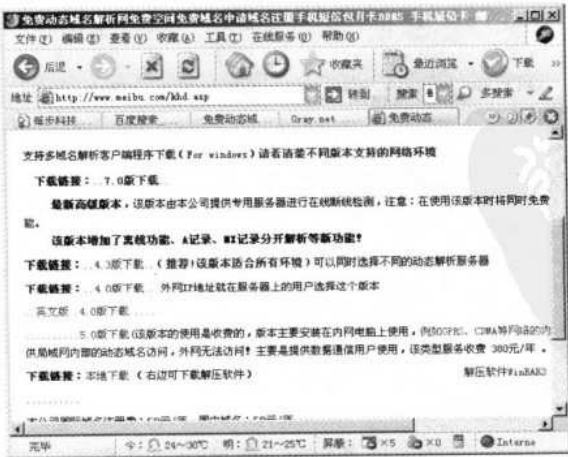


图 1-20 每步动态域名解析客户端软件下载界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这里“支持单域名解析”和“支持多域名解析”的客户端版本功能相同，只不过后者允许在同一台计算机上供 3 个用户使用，每个用户都可使用自己注册的不同域名，所以就具有多域名功能。

2. 客户端的登录

安装好相应的客户端软件后，即可利用客户端软件登录到每步数码公司的网站，以提供动态域名解析服务。单机版和多用户版的设置界面和功能基本一致，唯一不同的是多用户版可以选择多个不同用户登录，从而达到在单机上使用多域名的功能。如图 1-21 所示的是 1.0 版本的客户端软件用户登录界面，客户端的设置非常简单，只需填入注册获得的用户名和密码，单击【登录】即可。如果连接成功，会有“IP 改变，正在登录”状态提示，如图 1-22 所示。

如图 1-23 所示的是 4.3 版本的客户端登录界面，在这个界面中可以选择登录的服务器，当选择某个服务器登录失败时，可以选择另一个。登录成功后同样会有“IP 改变，正在登录”的状态提示，如图 1-24 所示。

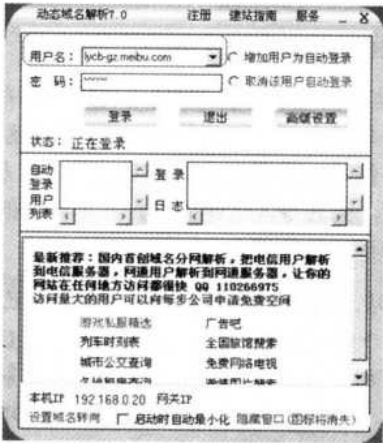


图 1-21 1.0 版客户端登录界面

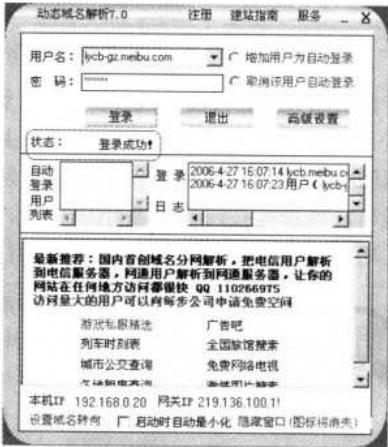


图 1-22 1.0 版客户登录成功后的系统状态提示

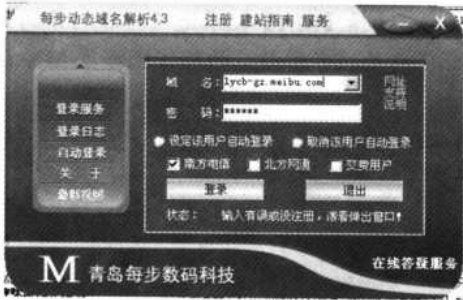


图 1-23 4.3 版客户端登录界面

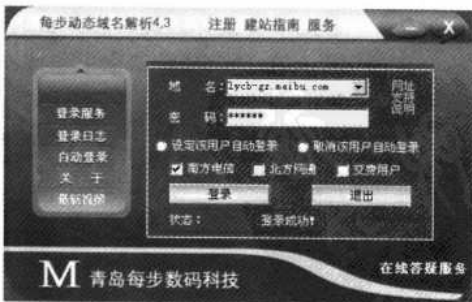


图 1-24 4.3 版客户端登录成功后的状态提示

不过，需要注意的是，这里所使用的登录账户不再像在网域科技公司中申请的护照那样，而是直接采用申请的域名，如本例的 lymb-gz.meibu.com。

16 网管员必读——网络应用（第2版）

在正式对外发布网页之前，还需要检测一下每步域名解析的正确性。在 Windows 98 系统下可以很方便地使用 Ping 和 Winipcfg（Windows 2000 以上版本用 Ipconfig /all 命令）命令来测试每步对 DNS 域名的解析是否与目前主机的动态 IP 地址一致。例如注册了“lycb-gz.meibu.com”的免费域名，则可在提示符窗口下输入“ping lychb-gz.meibu.com”，Ping 命令反馈的 IP 地址（如图 1-25 所示）应该与使用 Winipcfg（或者 Ipconfig /all）所查看到的系统主机当前 IP 地址一致（必须在主机直接接入互联网情况下测试）。如果确认两者相同，则表明每步的动态域名解析已经处在正常运行状态下。



图 1-25 Ping 所申请的域名显示结果

目前各种动态域名解析软件一般仅支持公网 IP 地址的域名解析，对使用局域网具有私网 IP 地址的用户支持不够。一个解决办法是在网关上搭建动态域名解析软件，另一个办法是使用代理服务器。另外目前很多动态域名解析软件的工作不太稳定，解析速度、稳定性方面还有待提高，重新连接时也容易出现串号、断线等问题，尤其令人遗憾的是，完全免费的软件不多且功能有所限制，提供的免费域名往往是二级甚至三级的域名。



如果把所申请的域各用于 Web 网站、FTP 站点，则可以直接在自己的网站上配置即可，如果把所申请的域名用于邮件服务器，则需要通知提供 DDNS 服务的相应服务商，把邮件服务器对应的邮件域名 MX 记录添加到服务商的 DNS 服务器上，否则邮件服务器不能正常运行。这一点就与局域网中 DNS 服务器要添加邮件服务器 MX 记录一样。网域科技公司新版本的花生壳客户端软件可以允许用户自己添加 MX 记录，方法是在如图 1-14 登录界面上显示的域名上单击鼠标右键，在弹出的快捷菜单中选择【MX】记录选项，在打开的如图 1-26 所示的对话框中即可添加自己申请的域名所对应的邮件服务器 MX 记录。



图 1-26 在“域名管理”窗口添加邮件服务器 MX 记录

1.3 端口映射

若网站服务器是直接连接互联网的，则无须其他配置了，通过本章前面所讲的配置就可把单位的网站放在互联网上供大家访问了。但如果网站服务器是通过路由器、代理服务器这样非直接互联方式，则需要进行端口映射了，否则个别用户无法访问这公司的网站了。

端映射其实就是通常所说的 NAT（网络地址翻译），它是将公网 IP 翻译成私有地址。这里涉及到的端口映射种类主要有 3 种：代理服务器上的端口映射；路由器上端口映射；支持路由的 ADSL MODEM 上的端口映射。本节要分别予以介绍。

1.3.1 宽带路由器上的端口映射

端口映射其实就是常说的 NAT 地址转换的一种，其功能就是把在公网的地址转译成私有地址。采用路由方式的 ADSL 宽带路由器拥有一个动态或固定的公网 IP，ADSL 直接接在 HUB 或交换机上，所有的电脑共享上网。这时 ADSL 的外部地址只有一个，比如 202.96.168.68。而内部的 IP 是私有地址，比如宽带路由器的 IP 地址设为 192.168.0.1。

现在用宽带路由器共享上网的用户是最多的了，因为它为共享上网提供了便利，不用像代理服务器那样，先启用一台代理服务器，也不占用一台主机。如果企业网站也是通过路由器共享上网，则必须在宽带路由器上配置端口映射。现在以 TP-LINK 的 TL-WR541G 型号无线宽带路由器为例进行介绍，其他型号的参照即可。

(1) 首先了解相应宽带路由器上设置的 IP 地址，如 TL-WR541G 型号无线宽带路由器的出厂设置是 192.161.1.1。把宽带路由器用一条直通线直接连接主机网卡，并把主机网卡 IP 地址设置与宽带路由器在同一网段中。

(2) 打开浏览器，在浏览器地址栏中输入宽带路由器 IP 地址，如笔者的 TL-WR541G 型号宽带路由器的 IP 地址为 192.161.1.1，首先打开的是如图 1-27 所示身份验证对话框。在这里输入进入配置界面的用户账户信息。宽带路由器在出厂时都有默认设置，如 TP-LINK 公司基本上都是用户名和密码均为“admin”。输入后单击【确定】按钮即可进入宽带路由器配置主界面，如图 1-28 所示。

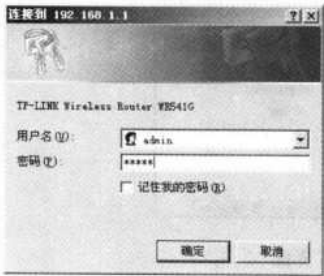


图 1-27 进入宽带路由器配置界面的身份验证对话框

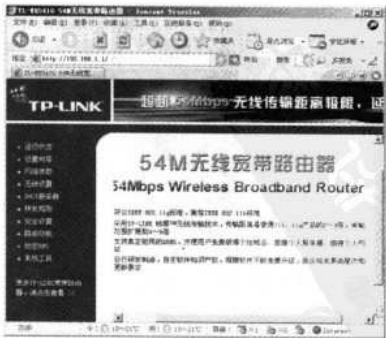


图 1-28 DI-604+宽带路由器配置主界面

18 网管员必读——网络应用（第2版）

(3) 在界面左边导航栏中单击【转发规则】按钮，然后在展开的导航栏中单击【虚拟服务器】按钮，打开如图 1-29 所示配置界面。在“服务端口”文本框中输入 Web 服务器中 WWW 服务所用端口 80；在“IP 地址”文本框中输入 Web 服务器的 IP 地址(如 192.168.1.100)；在“协议”下拉列表中选择“TCP”选项（或者选择默认的“all”选项），然后选择后面的“启用”复选项。

如果内网中的互联网服务器是 FTP 服务器，由于 FTP 服务器用到了 20 和 21 两个 TCP 端口，所以，要把以上两个端口都添加在图 1-29 所示界面，配置的方法与 80 号 WWW 端口一样。



图 1-29 端口映射配置界面

(4) 配置好后，单击【保存】按钮，重新启动宽带路由器即可生效。

对于公众互联网服务器，则建议把公众服务器放在宽带路由器所带的防火墙的 DMZ 区域，这样用户访问起来更加容易。配置方法也很简单，只需在如图 1-29 所示配置界面左边导航栏中单击【DMZ 主机】按钮，打开如图 1-30 所示配置界面。

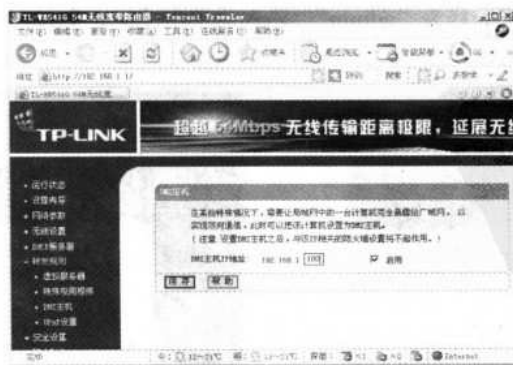


图 1-30 DMZ 主机配置界面

在“DMZ 主机 IP 地址”栏中填上要放在 DMZ 中的互联网服务器 IP 地址，然后选择“启

用”复选项。单击【保存】按钮保存设置。重启路由器后生效（注意：放置在 DMZ 中的主机不再享受宽带路由器的防火墙设置）。

最后介绍一些宽带路由器上的 DDNS 设置，因为目前许多宽带路由器都已支持 DDNS，这样也就无须在互联网服务器端安装、运行 DDNS 客户端软件。如笔者的 TL-WR541G 无线宽带路由器就支持 DDNS，不过一般的宽带路由器只支持两种左右 DDNS 服务商提供的动态域名解析，如本章前面介绍的网域科技的“花生壳”DDNS 和科迈公司的动态域名解析。

TL-WR541G 无线宽带路由器的 DDNS 配置只需在如图 1-30 所示配置界面左边导航栏中单击【动态 DNS】按钮。在打开的对话框“服务提供商”下拉列表中可选择以上两个 DDNS 服务提供商，如图 1-31 是选择网域科技的“花生壳”DDNS 服务的配置界面，只需在其中配置所申请的护照名和密码，然后选择“启用 DDNS”复选项，单击【保存】按钮保存设置。最后单击【登录】按钮即自动使用所配置的护照在网域科技公司的 DDNS 服务器上登录，以启用 DDNS 服务。

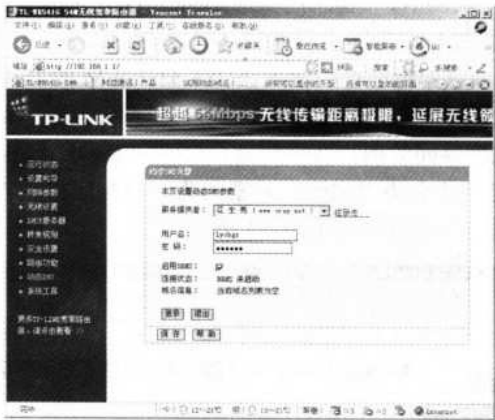


图 1-31 选择“花生壳”时的 DDNS 配置界面

如果在“服务提供商”下拉列表中选择是“科迈网”动态域名解析服务，则配置界面如图 1-32 所示。



图 1-32 选择“科迈网”时的 DDNS 配置界面

20 网管员必读——网络应用（第2版）

然后配置所申请的动态域名和账户信息。再选择“启用 DDNS”复选项即可，单击【保存】按钮保存设置，最后单击【登录】按钮使用所输入的账户信息登录到相应 DDNS 服务商的 DDNS 服务器网络中。

1.3.2 ADSL MODEM 上的端口映射

因为路由共享上网方式给人们提供了很大的便利，所以现在的 ADSL MODEM 也基本上都会附带基本的路由功能，如果企业的 Web 网站是直接这样的 ADSL MODEM 共享上网，那又该如何配置呢？在此以笔者的伊泰克 2001 ADSL MODEM 为例向大家介绍，其他的参照即可。

(1) 首先要了解相应 MODEM 上设置的 IP 地址，如笔者的 etek-2001 型号 ADSL MODEM 的出厂设置是 192.161.1.1。把 ADSL MODEM 用一条直通线直接连接 Web 服务器网卡（此时 Web 服务器上要多加一块网卡，一块用于与 ADSL MODEM，另一块用于与局域网连接），并把主机网卡 IP 地址设置成与宽带路由器在同一网段中。

(2) 打开浏览器，在浏览器地址栏中输入 ADSL MODEM 的 IP 地址，如笔者的 etek-2001 型号的 ADSL MODEM 的 IP 地址为 192.168.1.1，首先打开的也是如图 1-27 所示身份验证对话框。在这里输入进入配置界面的用户账户信息。ADSL MODEM 在出厂时也都有默认设置，如伊泰克公司基本上都是用户名为“admin”，密码为“12345”。输入后单击【确定】按钮即可进入 ADSL MODEM 配置主界面，如图 1-33 所示。

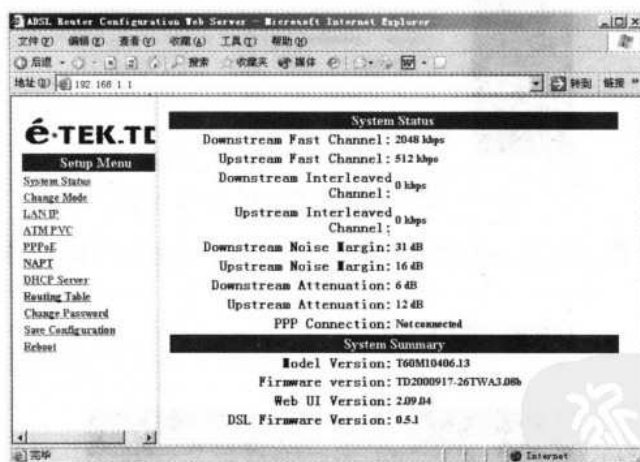


图 1-33 ADSL MODEM 配置主界面

(3) 在左边导航栏中选择“NAPT”选项，打开如图 1-34 所示配置界面。在“Interface”下拉列表中选择 Web 服务器上用于连接交换机的网卡，在“PortNum”文本框中输入 WWW 服务专用端口号 80（这是默认的 www 服务端口，不要改变），在“Protocol”下拉列表中选择“TCP”选项；在“Server IP Address”栏中输入 Web 网站服务器的 IP 地址。

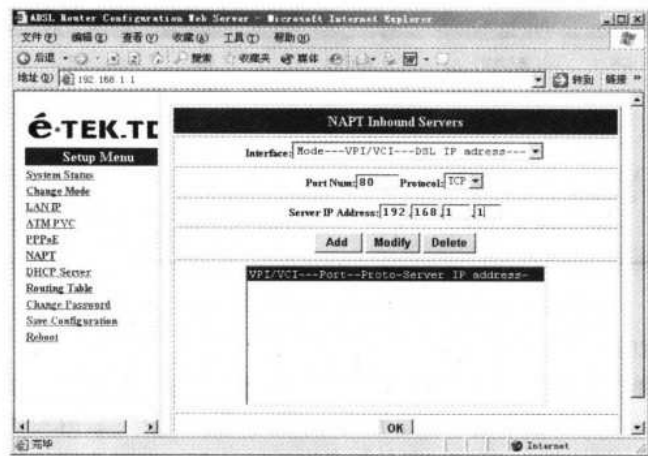


图 1-34 配置端口映射的 NAPT 界面

(4) 单击【Add】按钮即可把以上配置项添加到下面的列表中，完成了 www 服务端口映射配置过程。重新启动 MODEM 即生效。

1.3.3 代理服务器上的端口映射

如果互联网服务器不是通过路由器共享上网的，而是通过代理服务器上上网的，则需要通过专门的端口镜像软件做端口映射（不过，也有些代理服务器软件本身就有端口镜像功能，如 CCProxy，此时就用专门的端口镜像软件了）。目前笔者认为比较好用的端口映射软件是 Port Tunnel（目前最新版本为 2.0.15.347）。本节介绍这款软件的端口映射配置方法。下面提供两个下载地址：

- http://www.steelbytes.com/download/PortTunnel_CH.zip（中文）
- http://www.steelbytes.com/download/PortTunnel_ENGUK.zip（英文）

下载后还不能立即安装，因为它需要微软的 .NET Framework 2.0 以上版本支持才可进行安装，否则会出现如图 1-35 所示提示框。单击【是】按钮自动从微软的官方网站下载。也可直接到微软的官方网站上下载：

<http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=zh-cn>

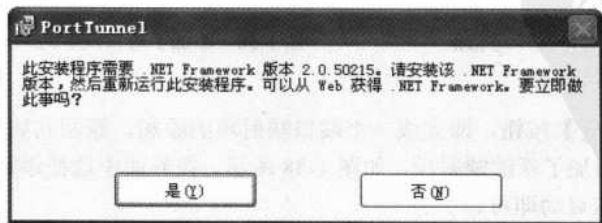


图 1-35 没有安装.NET Framework 2.0 以上版本前安装 Port Tunnel 时出现的错误提示
安装好后，运行 Port Tunnel 程序，出现如图 1-36 所示主界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

22 网管员必读——网络应用（第2版）

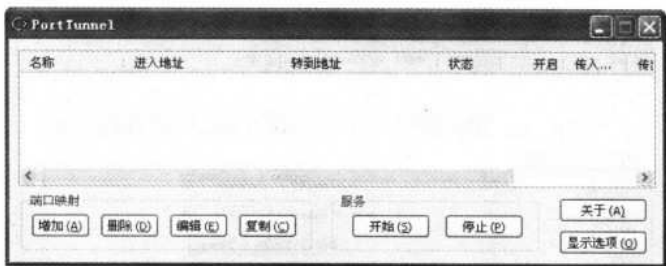


图 1-36 Port Tunnel 主界面

配置端口映射的方法很简单，具体方法如下。

(1) 单击【增加】按钮，在打开的对话框中选择“常规”选项卡，如图 1-37 所示。

(2) 在“名称”文本框中输入新建的端口映射名称，选择“启用”复选项，在“对外”栏中的“端口”文本框中输入 WWW 服务的专用端口号 80（此时选择的是“单一”单选项，也可以通过选择“范围”单选项，把外网中一个范围内的端口都映射到本地机的某个端口上）；在“映射到”栏中的“端口”文本框中输入 Web 网站服务器的 WWW 服务端口号，一般也为 80。然后在“目标地址”文本框中输入 Web 网站的网址，如笔者申请的为 lycbqx.xicp.cn。其他按系统默认配置即可。



图 1-37 “新建端口映射”对话框
“常规”选项卡

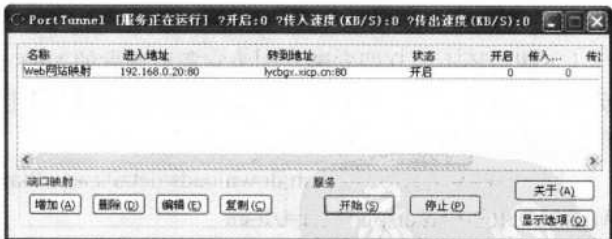


图 1-38 添加了端口映射的 Port Tunnel 主界面

(3) 单击【确定】按钮，即完成一个端口映射项的添加，返回到如图 1-36 所示程序主界面，不过此时已添加了新的映射项，如图 1-38 所示。在界面中选择添加的端口映射项，然后单击【启动】按钮启动即可。

至于如图 1-37 所示的对话框的“其他”选项卡，可根据实际需要选择配置，一般情况下只需按以上配置即可。

总结：经过以上配置，所有网络连接方式下的动态域名解析配置工作就完成了，网站制

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

作并配置好后就可以利用自己申请的动态域名解析服务，在互联网上架设自己的网站了。如图 1-39 所示就是笔者利用在网域科技公司申请的 lycbgz.xicp.net 域名架设的动态网站，其中网站服务器是通过宽带路由器共享 ADSL PPPoE 拨号线路上网的。网站是由 IIS 制作的，具体参见下章介绍。



图 1-39 动态域名解析网站示例

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第 2 章 IIS 6.0 Web 网站配置与管理

随着网络技术的不断发展和互联网应用的不断深入、普及，网站已经深入应用到企业，甚至个人中了。而且建站的方法也是越来越容易，一步步趋向傻瓜型。

网站建设的方法有多种，但目前应用最广，最受用户欢迎的仍是微软 Windows 系统自带的 IIS 方案，以及在 Windows、UNIX、Linux 平台中都可采用的 Apache Server 方案。随着微软 IE 7.0 的推出，IIS 方案更加成熟，更加专业，解决以前版本中存在的许多性能和安全方面的问题，得到了用户的高度认可。在新的 Windows Server 2003 R2 版本系统中，IIS 不仅可以组建普通的网站，还自带了诸如 SharePoint 站点和 Windows Media Services 站点，使得 IIS 在站点组建方面的应用领域更加广泛。

基于篇幅原因，本章仅向大家介绍目前应用最广的 Windows Server 2003 系统 IIS 6.0 方案。本章注重网站建设思路的介绍，使读者阅读和理解起来更轻松，操作性更强。

本章重点

- IIS 6.0 网站建设的基本思路
- IIS 6.0 相对以前版本的更改
- IIS 6.0 的主要安全措施
- IIS 6.0 隔离模式工作原理，与 IIS 5.0 隔离模式的区别
- 利用向导法创建新网站的方法
- 网站基本信息配置方法
- 网站身份验证配置方法
- 虚拟目录的创建与配置
- 网站的性能管理
- 网站的服务质量管理
- 网站的远程管理

2.1 利用 IIS 6.0 组建网站的基本思路

为了使大家对利用 IIS 组建网站的方法有一个大致的了解，增强组建网站的信心，在这一节介绍利用 IIS 6.0 组建网站的基本思路。随后的内容也是按照这个思路叙述的。

本章用了大量篇幅进行系统介绍，以及全面的配置方法。特别是网站安全方面的配置，在实际中，往往只需选择其中的一两种进行配置即可，没有必要进行全面配置。

利用 IIS 6.0 组建网站的基本思路如下。

1) 安装并启用 IIS 和相关组件

这一步是前提，否则在网站建设中所需要用到的“Internet 信息服务（IIS）管理器”就不会在系统中出现，我们也就无法使用它来建设网站了。

但要注意，组建一个功能全面、专业的网站，仅安装了基本的 IIS 组件是不够的，还应安装其他一些服务，或管理工具组件，如网页支持语言 ASP、ASP.NET、NET FRAME，以及远程管理（HTML）等。对于像 ASP、ASP.NET、Web DAV 等扩展服务，有时还需要特意启用，否则即使安装了，网站也可能不支持 ASP、ASP.NET 等网页，或者不支持网站的远程管理了。

IIS 及相关组件的具体安装方法参见 2.2 节。

2) 新建网站（可选）

新建网站是在 IIS 管理器中进行的。网站的新建可以采取两种方式：一是编辑系统自带的“默认网站”，二是重新利用向导新建。如果公司只需一个网站，建议采用编辑系统默认网站（但不能是用于管理的 Administrator 网站、Windows SharePoint Services 和 Windows Media Services 网站）方式，所以此步为可选项。

网站的具体新建步骤参见 2.3 节。

3) 网站的基本配置

网站的基本配置包括以下两个主要方面。

■ 网站基本信息配置。

如果是采用向导方式新建网站，这一步可略过，但也可以通过此步骤重新配置。如果采用的是编辑现有网站的方式新建网站，则必须经过这一步。在这一步就需要为我们新建的网站取一个好记，且有代表性的名称，选择所用的 IP 地址和端口，并且把网站与域名对应起来，也就是配置网站的主机头值。这些都是最基本的网站标识信息，是网站能否正常被访问的最基本配置，否则 IIS 系统无法准确定位所建设的网站，用户也就无法打开网站了。

■ 指定网站主目录和主页文件。

安装了 IIS 和相关组件后，就可以利用“Internet 信息服务（IIS）管理器”把网站文件集中管理起来。首先要确定好一个用来存放网站文件的文件夹，也就是网站的主目录（至于服务器性能方面的选择在此就不多介绍了，参见笔者的《网管员必读——服务器与数据存储》一书即可）。

在选择主目录时一方面要考虑所对应的磁盘分区空间大小是否能满足网站当前和未来相当长一段时间的发展需求，另一方面要选择 NTFS 格式的磁盘分区，这是出于安全考虑的，因为 NTFS 格式文件可以设置用户的访问权限，而 FAT 格式不行。

网站文件放入主目录中后，还得在 IIS 管理器中设定好。并且还要设置好网站的默认主页，这样用户在访问网站时无须输入具体的网页文件名就可以直接访问了。

以上两个方面的配置过程将在 2.4 节具体介绍。

4) 网站的安全配置

网站的安全配置也包括两个方面：网站的身份验证方式和网站的访问权限，当然还可能包括其他安全配置，如 IP 地址过滤、网站过滤和服务器证书等。具体包括如下。

■ 配置身份验证方式。

这一步是为网站系统指定一种用户身份验证的方式。非常关键，也非常重要，因为它关系到网站的安全和允许用户的访问权限。在 IIS 中提供了多种身份验证方式，最简单的就是匿名访问方式，也就是无须进行身份验证，以最低级别的读取方式访问网站。还有以 Windows 系统账户集成的身份验证方式、密码验证方式、域账户身份验证方式等。不同的身份验证方式所需要的系统支持也不一样。如域账户身份验证方式就只能在域网络中进行。

■ 配置用户的网站访问权限及其他安全选项。

上一步是指定一种用户访问网站时的身份验证方式，本步主要针对非匿名访问方式下的用户访问权限。它是直接针对网站主目录下的文件夹和文件进行的 NTFS 权限设置。

至于其他的一些网站安全选项，可根据实际的需要选择配置，如网站所采用的隔离方式、服务器证书、IP 和网站的过滤等。

以上配置步骤将在 2.5 节具体介绍。

一般的企业内部网站，只需配置以上的四项即可，下面的选项配置不是必须进行的。

5) 创建和配置虚拟目录（可选）

虚拟目录也并不是所有网站都需要的，只是在网站有网页文件不在网站主目录下时才需要创建和配置。

具体创建与配置的过程将在 2.6 节介绍。

6) 网站管理（可选）

此处所介绍的网站管理事项具体包括如下两个方面。

■ 网站性能管理。

在网站性能管理方面，主要可配置网站允许使用的最高带宽值和最大并发连接数。

■ 服务质量管理。

网站的服务质量管理包括最大连接数、连接带宽、HTTP 压缩、连接超时、CPU 监视等。

■ 其他管理选项。

这里所说的其他管理选项可以是以上没有说到所有选项，如 HTTP 头、内容分级、网站有效期、ISAPI 期筛选、网站错误定义等。

以上选项配置过程参见 2.7 节。

7) 配置端口镜像和动态域名服务（可选）

如果所建的 Web 网站是对外服务的，不限于局域网用户，而且 Web 服务器不是直接与

28 网管员必读——网络应用（第2版）

外网连接的，而是通过共享方式上网的（如代理服务器共享上网、路由器共享上网和网关服务器共享方式等），此时就需要在路由器、代理服务器，或者专门的端口镜像软件上配置好 Web 服务器的端口镜像，否则外网用户无法访问 Web 网站。如果仅用于局域网内部用户访问，或者 Web 服务器直接连接互联网，则不用配置端口镜像。

另外，如果对外网用户服务器的 Web 网站，没有固定的公网 IP 地址（采用拨号上网之类的用户），则需要采用动态域名解析服务（DDNS）了。此时在申请公网域名的同时需向有关的服务商申请动态域名解析。因为没有固定的公网 IP 地址，域名就无法与 IP 地址形成一一对应的关系，如果再没有 DDNS，用户访问域名也就无法打开网站。

2.2 安装并启用 IIS 及相关组件

在 Windows Server 2003 R2 版本系统中的 IIS 6.0 与以前版本存在较大区别，所以在正式介绍 IIS 及相关组件的安装和启用方法之前，有必要先对这一系统中的 IIS 6.0 基础知识有一个基本了解。

2.2.1 IIS 6.0 的主要更改

IIS 6.0 包括许多新功能，它们旨在帮助企业、IT 专业人士和 Web 管理员（他们可能拥有位于单个 IIS 服务器或多个服务器上的数千个网站）实现其网站在性能、可靠性、可伸缩性和安全性方面的目标。表 2-1 总结了不同版本 IIS 之间的重要区别。

表 2-1 不同版本 IIS 之间的重要区别

	IIS 4.0	IIS 6.0	IIS 2.1	IIS 6.0
平台	Windows NT 4.0	Windows 2000	Windows XP Professional	Windows Server 2003 家族
体系结构	32 位	32 位	32 位和 64 位	32 位和 64 位
应用程序进程模型	TCP/IP 内核 MTX.exe	TCP/IP 内核 DLLhost.exe（处于中等或高应用程序隔离模式下的多个 DLL 主机）	TCP/IP 内核 DLLhost.exe（处于中等或高应用程序隔离模式下的多个 DLL 主机）	HTTP.sys 内核。当 IIS 以 IIS 6.0 隔离模式运行时采用 Inetinfo.exe（对于进程内应用程序）或 DLLhost.exe（对于进程外应用程序）；当 IIS 以工作进程隔离模式运行时采用 W3wp.exe（多工作进程）
数据库配置	二进制	二进制	二进制	XML
安全性	Windows 身份验证、SSL	Windows 身份验证、SSL、Kerberos	Windows 身份验证、SSL、Kerberos 和安全向导	Windows、身份验证、SSL、Kerberos、安全向导和 Passport 支持
远程管理	HTMLA	HTMLA	无 HTMLA，采用终端服务	远程管理（HTML）和终端服务
群集支持	在 Windows NT 系统中	IIS 群集	Windows 支持	Windows 支持
WWW 服务	Windows NT 4.0 上的 IIS	Windows 9x 上的个人 Web 管理器，Windows 2000 上的 IIS	（可选）Windows XP Professional 上的 IIS	Windows Server 2003 家族成员上的 IIS

2.2.2 IIS 6.0 提供的服务

IIS 6.0 提供了基本服务，包括发布信息、传输文件、支持用户通信和更新这些服务所依赖的数据存储。表 2-2 列出了 IIS 6.0 所提供的服务及其主要组件和服务宿主。

表 2-2 IIS 6.0 提供的服务及其主要组件和服务宿主

服 务	主 要 组 件	宿 主 于
万维网发布服务（WWW 服务）	Iisw3adm.dll	Svchost.exe
文件传输协议服务（FTP 服务）	Ftpsvc.dll	Inetinfo.exe
简单邮件传输协议服务（SMTP 服务）	Smtpsvc.dll	Inetinfo.exe
网络新闻传输协议服务（NNTP 服务）	Nntpsvc.dll	Inetinfo.exe
IIS 管理服务	Iisadmin.dll	Inetinfo.exe

1) 万维网发布服务

通过将客户端的 HTTP 请求连接到 IIS 中运行的网站上，万维网发布服务（WWW 服务）向 IIS 最终用户提供 Web 发布。万维网发布服务管理 IIS 核心组件，这些组件处理 HTTP 请求并配置和管理 Web 应用程序。

万维网发布服务是以 Iisw3adm.dll 链接文件形式运行并宿主于 Svchost.exe 中的。

2) 文件传输协议服务

通过文件传输协议服务（FTP 服务），IIS 提供对管理和处理文件的完全支持。该服务使用传输控制协议（TCP），这就确保了文件传输的完成和数据传输的准确性，因为它是一个面向连接的传输层协议。该版本的 FTP 支持在站点级别上隔离用户，以帮助管理员保护其 Internet 站点的安全，并使之商业化。

FTP 服务是以 Ftpsvc.dll 链接文件形式运行并宿主于 Inetinfo.exe 中的。

3) 简单邮件传输协议服务

通过使用简单邮件传输协议服务（SMTP 服务），IIS 能够发送和接收电子邮件。例如，为确认用户提交表格成功，可以对服务器进行编程以自动发送邮件来响应事件。也可以使用 SMTP 服务以接收来自网站客户反馈的消息。SMTP 不支持完整的电子邮件服务。要提供完整的电子邮件服务，需要使用 Exchange Server。

SMTP 服务是以 Smtpsvc.dll 链接文件形式运行并宿主于 Inetinfo.exe 中的。

4) 网络新闻传输协议服务

可以使用网络新闻传输协议服务（NNTP 服务）主控单个计算机上的 NNTP 本地讨论组。因为该功能完全符合 NNTP 协议，所以用户可以使用任何新闻阅读客户端程序加入新闻组进行讨论。通过 Inetsrv 文件夹中的 Rfeed 脚本，IIS NNTP 服务现在支持新闻流，但 NNTP 服务不支持复制。要利用新闻流或在多个计算机间复制新闻组，需要使用 Exchange Server。

NNTP 服务是以 Nntpsvc.dll 链接文件形式运行并宿主于 Inetinfo.exe 中。

5) IIS 管理服务

IIS 管理服务管理 IIS 配置数据库，并为 WWW 服务、FTP 服务、SMTP 服务和 NNTP 服务更新 Windows 操作系统注册表。配置数据库是保存 IIS 配置数据的数据存储。IIS 管理服务对其他应用程序公开配置数据库，这些应用程序包括 IIS 核心组件、在 IIS 上建立的应用程序及独立于 IIS 的第三方应用程序（如管理或监视工具）。

30 网管员必读——网络应用（第2版）

IIS 管理服务是以 `Iisadmin.dll` 链接方式形式运行并宿主于 `Inetinfo.exe` 中的。

2.2.3 IIS 6.0 的核心组件

IIS 6.0 核心组件由内核模式进程和用户模式进程组成。具体包括以下几个方面。

- **HTTP.sys**：将 HTTP 请求传送到用户模式应用程序的内核模式设备驱动程序。
- **WWW 服务管理和监视组件**：配置“万维网发布服务”，并管理工作进程。
- **工作进程**：处理提交到分配给它们的 Web 应用程序的请求。
- **Inetinfo.exe**：主控配置数据库和非 Web 服务。

1. HTTP.sys

超文本传输协议（HTTP）侦听程序作为 HTTP.sys 的内核模式设备驱动程序。HTTP.sys 是 Windows 网络子系统的一部分，被用做 IIS 6.0 的一个核心组件。

通过把 HTTP.sys 作为内核模式组件来运行，IIS 6.0 提供了下面两种增强的性能（但在把 HTTP 侦听程序作为用户模式运行时并不包含这两种增强的性能）。

- 通过直接分派给来自内核的正确进程，处理请求只需要较少的上下文切换开销。
- 通过启用内核模式缓存，无须切换到用户模式即可处理缓存的返回请求。

HTTP.sys 的工作原理可以描述如下。

当在 IIS 中创建网站时，使用 HTTP.sys 注册站点，然后 HTTP.sys 将 Web 请求传送到正在运行网站的用户模式进程中。HTTP.sys 也将响应送回客户端，除了从其内部缓存中检索存储的响应以外，HTTP.sys 并不处理它所接收到的请求。因此，应用程序特定代码永远不会加载到内核模式中。这使得应用程序特定代码错误不会影响到内核模式进程或导致系统故障。

HTTP.sys 还提供了 IIS 使用的其他服务，包括内容如下。

- 管理传输控制协议（TCP）连接。
- 将 HTTP 请求传送到正确的请求队列中。
- 以内核模式缓存响应。
- 执行所有基于文本的 WWW 服务日志记录。
- 实现“服务质量”（QoS）功能，其中包括连接限制、连接超时、队列长度限制和带宽限制。

2. WWW 服务管理和监视组件

WWW 服务管理和监视是“万维网发布服务”（WWW 服务）的新组件，负责任务和进程管理。在管理角色下，WWW 服务管理和监视将实现 WWW 服务的服务控制功能；与配置数据库交互，以获得传递给 HTTP.sys，或在管理工作进程时所使用的配置数据；支持剩余运行时服务管理。在管理任务下，WWW 服务管理和监视负责管理工作进程，其中包括启动工作进程及维护其在运行时的信息。

WWW 服务管理和监视组件是以用户模式在非共享的 `svchost.exe` 文件下运行的，而且是作为 LocalSystem 进程运行的。

3. 工作进程

工作进程是以用户模式运行的应用程序。它的一般角色包括处理请求以返回静态界面、

调用 Internet 服务器 API (ISAPI) 扩展或筛选器，或运行通用网关接口 (CGI) 处理程序。工作进程在物理上被实现名为 W3wp.exe 的可执行文件，并由“WWW 服务管理和监视”组件进行控制。

在默认情况下，IIS 6.0 的工作进程作为 NetworkService 来运行，这使之具有与所需要的功能相兼容的最强安全性（最少的访问权）。工作进程使用 HTTP.sys 用于在 Web 上发送请求和接收响应。工作进程也运行应用程序代码，如 ASP.NET 应用程序。根据 IIS 的配置情况，可以有多个运行的工作进程来同时处理不同的 Web 应用程序。这种设计通过进程边界将应用程序隔离起来，并有助于实现 Web 服务器的最大可靠性。

4. Inetinfo.exe

Inetinfo.exe 是主控 IIS 6.0 组件，而非像 WWW 服务的用户模式组件。这些组件包括文件传输协议服务 (FTP 服务)、简单邮件传输协议服务 (SMTP 服务)、网络新闻传输协议服务 (NNTP 服务) 和 IIS 配置数据库。Inetinfo.exe 也可主控当 IIS 6.0 处于 IIS 5.0 隔离模式下时运行的单个工作进程。



在 IIS 6.0 中，运行在 Inetinfo.exe 中的服务使用 LocalSystem 标识（运行服务时的账户）作为 DLL 文件运行。因为使用该账户可以获得对本地计算机上实际每个资源的访问权，所以应小心使用 LocalSystem 账户，特别是在 Internet 上提供服务的计算机。

2.2.4 安装 IIS 及相关组件

在 Windows Server 2003 R2 系统（建议采用这一系统，而不要采用 Windows XP 系统，因为 Windows Server 2003 R2 系统性能更好，安全性更高）安装 IIS 6.0 及相关组件的方法有 3 种：（1）通过“配置你的服务器向导”进行；（2）通过控制面板中的“添加/删除程序”进行；（3）采用无人参与安装方式进行。不过在这里都要是系统管理员组（包括域管理员组）成员，或者已委派了相应权限的用户才能进行。下面分别予以介绍。

1. “配置你的服务器向导”方式

这是一种通用的服务器配置方式，包括域控制器、DNS、DHCP、WINS 服务器，以及其他一些应用服务器等都可以通过这个向导进行安装。但是利用这种方法安装 IIS 及相关组件并不是很好，因为还有些组件并不包括在其中，安装后可能还得重新利用控制面板中的“添加/删除程序”来添加安装。这一安装方法的具体步骤如下。

（1）执行【开始】→【管理员】→【配置你的服务器向导】菜单操作，打开如图 2-1 所示的对话框。

32 网管员必读——网络应用（第2版）

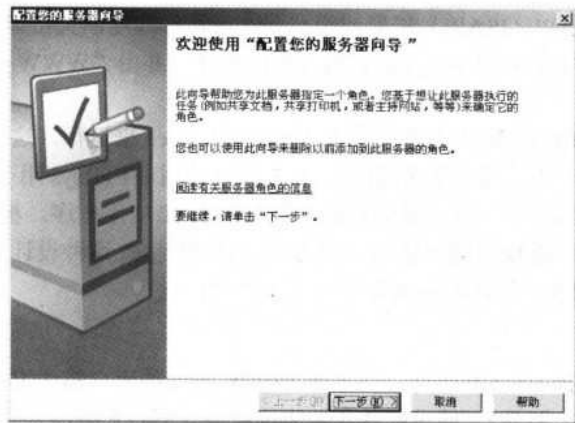


图 2-1 “欢迎使用‘配置你的服务器向导’”对话框

（2）单击【下一步】按钮，打开如图 2-2 所示的对话框。在这里显示要进行下面的向导操作需要做好的准备工作，对照检查一下，否则向导可能无法向下进行。

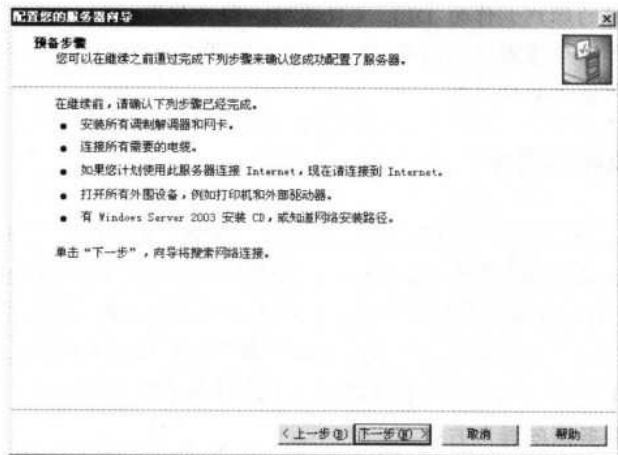


图 2-2 “预备步骤”对话框

（3）单击【下一步】按钮，打开如图 2-3 所示的对话框。在这里选择“应用程序服务器（IIS，ASP.NET）”选项，然后继续单击【下一步】按钮，按向导提示即可很容易完成 IIS 组件的安装。

采用这一安装方式安装的 IIS，只是安装了 IIS 本身，以及 ASP、ASP.NET 等几个主要的组件，对于像“SharePoint”、“远程管理（HTML）”这类非必需组件就不安装了。而且在安装后，默认情况下同时启用 ASP.NET 服务扩展，这与下面的“添加/删除程序”方式不一样。

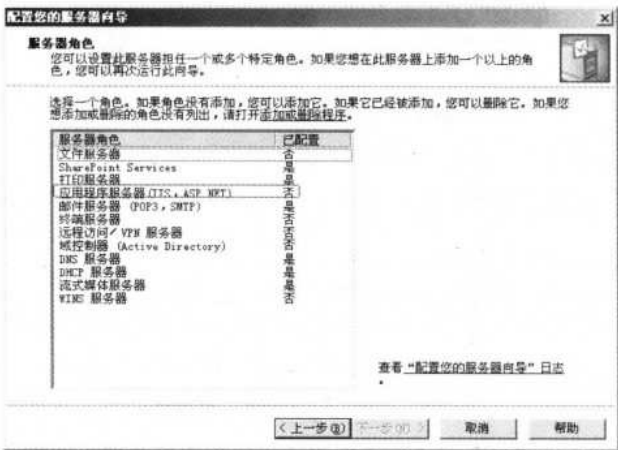


图 2-3 “服务器角色”对话框

2. “添加/删除程序”方式

利用控制面板中的“添加/删除程序”工具进行 IIS 及相关组件的安装方法很简单，而且也可以很全面。具体步骤如下。

(1) 执行【开始】→【控制面板】→【添加或删除程序】菜单操作，打开如图 2-4 所示窗口。

(2) 在界面左边导航栏中单击【添加/删除 Windows 组件】按钮，打开如图 2-5 所示的对话框。如果要在 IIS 管理器中同时显示 Windows SharePoint Services 和 Windows Media Services 站点，则要同时选择“Windows SharePoint Services”和“Windows Media Services”这两个组件项。



图 2-4 “添加或删除程序”界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

34 网管员必读——网络应用（第2版）

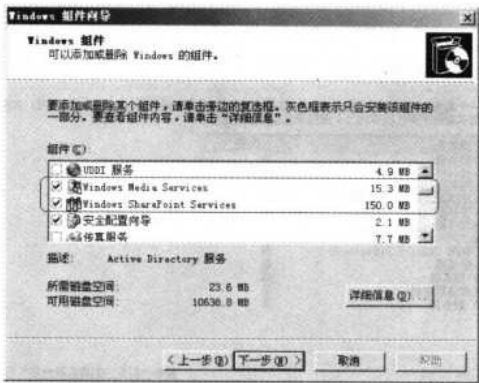


图 2-5 “Windows 组件”对话框

(3) 继续在如图 2-5 所示的对话框中选择“应用程序服务器”选项，如图 2-6 所示。再单击【详细信息】按钮，打开如图 2-7 所示的对话框。如果网站支持 ASP.NET，则首先要选择“ASP.NET”复选项。然后选择“Internet 信息服务 (IIS)”复选项。

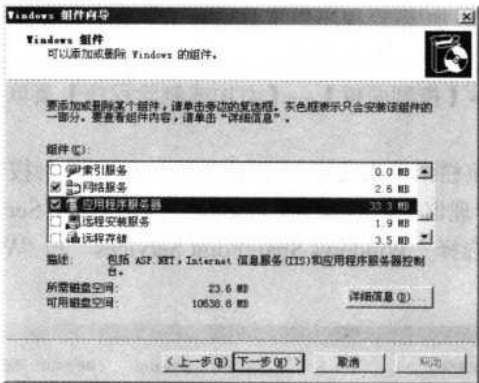


图 2-6 “Windows 组件向导”对话框

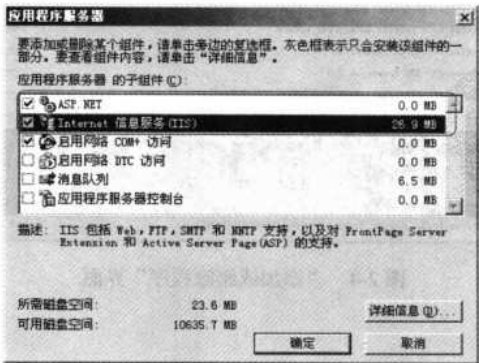


图 2-7 “应用程序服务器”对话框

(4) 选择“Internet 信息服务 (IIS)”复选项后，单击【详细信息】按钮，打开如图 2-8

所示的对话框。

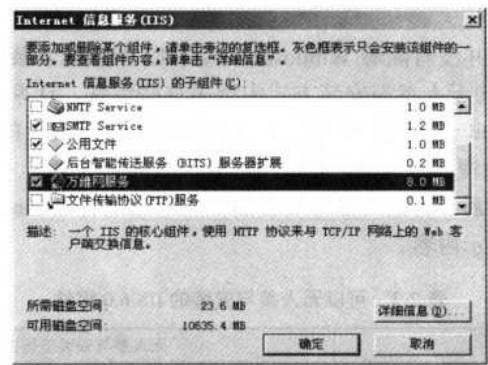


图 2-8 “Internet 信息服务 (IIS)” 对话框

在如图 2-8 所示的对话框中就可以选择很多需要安装的组件了，如 FrontPage 2002 Server 扩展（一般无须选择，因为现在用 FrontPage 制作网页的比较少）、Internet 信息服务管理器（要通过图形界面管理网站，则必须选择）、NNTP（网络新闻传输协议，配置新闻服务器时需要选用）服务、SMTP 服务（简单邮件传输协议，配置 POP3 邮件服务器时必须选择，此时可以不选择）、FTP 服务（文件传输协议，配置 FTP 站点时必须选择，此时可以不选择）等，根据实际需要选择。

（5）选择“万维网服务”复选项，单击【详细信息】按钮，打开如图 2-9 所示的对话框。在这里要同时选择“Active Server Pages”（以便支持采用 ASP 程序制作的网页）“万维网服务”和“远程管理（HTML）”（以便通过互联网远程管理网站服务器）3 个复选项。



图 2-9 “万维网服务”对话框

（6）选择好后，依次单击【确定】按钮，直到回到如图 2-6 所示的对话框。然后单击【下一步】按钮，系统会自动安装所选择的所有组件了。在安装时可能会提示插入 Windows Server 2003 R2 系统源程序光盘或指定磁盘位置。

通过以上步骤就可成功地安装 IIS 及所有相关组件，比前面介绍“配置你的服务器向导”方式更全面、更彻底。建议采用这一安装方式。不过，此种方式安装的 IIS，ASP 和 ASP.NET

36 网管员必读——网络应用（第2版）

都不是默认启用，需要专门启用，具体方法将在本章后面介绍。

3. 无人参与安装方式

虽然 IIS 及相关组件并没有随着 Windows Server R2 系统的安装而自动安装，但是可以在 Windows Server R2 系统的无人参与安装方式中部署这些组件，让系统自动选择安装。

为了简化运行 Windows Server 2003 家族成员的多台计算机上的 IIS 设置过程，可在无人参与的情况下运行安装程序。为此，创建并使用一个应答文件，该文件是一个自动回答安装问题的自定义脚本。然后，用无人参与安装的相应选项运行 Winnt32.exe。无人参与安装的 IIS 6.0 选项包括表 2-3 所示内容。

表 2-3 可以无人参与安装的 IIS 6.0 组件

组 件	无人参与安装应答文件中的.inf 参数
应用程序服务器	n/a (OCM 中的父对象)
ASP.NET #	aspnet = on/off
启用网络 COM+访问	complusnetwork = on/off
启用网络 DTC 访问	dtcnetwork = on/off
Internet 信息服务	n/a (OCM 中的父对象)
BITS 服务器扩展	n/a (OCM 中的父对象)
BITS 服务器扩展 ISAPI	bitsserverextensionsisapi = on/off
BITS 服务器扩展管理单元	bitsserverextensionsmanager = on/off
公用文件	iis_common = on/off
文件传输协议 (FTP) 服务	iis_ftp = on/off
FrontPage 2002 Server Extensions	fp_extensions = on/off
IIS 管理器	iis_inetmgr = on/off
NNTP Service	iis_nntp = on/off
SMTP Service	iis_smtp = on/off
万维网发布服务	n/a (OCM 中的父对象)
Active Server Pages	iis_asp = on/off
Internet 数据连接器	iis_internetdataconnector = on/off
远程管理 (HTML) *#	sakit_web = on/off
远程桌面 Web 连接	tswebclient = on/off
在服务器端的包含文件	iis_serversideincludes = on/off
WebDAV 发布	iis_webdav = on/off
WWW 服务	iis_www = on/off
应用程序服务器控制台 #	appsrv_console = on/off



表中带“*”的项必须在安装操作系统之后再通过控制面板中的“添加/删除程序”工具继续安装；表中带“#”的项在运行 Windows XP 64-Bit Edition、64 位版本的 Windows Server 2003 Enterprise Edition 或 Windows Server 2003 Datacenter Edition 的基于 Itanium（安腾处理器）的计算机上不可用。

具体的无人参与安装方法参见本系列丛书的《网管员必读——网络组建》一书。

无人参与安装方式，通过执行【开始】→【管理工具】→【Internet 信息服务管理器】（在

安装了“Internet 信息服务管理器”组件后才有该管理单元) 菜单操作后，即可打开 IIS 管理器，如图 2-10 所示。

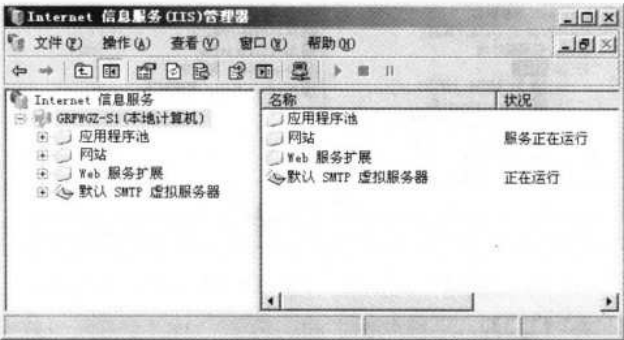


图 2-10 “Internet 信息服务 (IIS) 管理器”主界面

4. 扩展服务的启用

最后介绍一下相关服务的启用问题，因为采用“添加/删除程序”进行的 IIS 及相关组件安装方式时，所安装的 ASP、ASP.NET 等扩展服务是不默认启用的。具体的启用方法如下。

(1) 在 IIS 管理器控制台中首先要选择“Web 服务扩展”控制台树节点，在右边的详细信息窗口中即可查看“Active Server Pages”、“ASP.NET v1.1 和 ASP.NET 2.0”这 3 个扩展选项（当然还可以是其他扩展选项）是否处于“允许”状态，如图 2-11 所示。

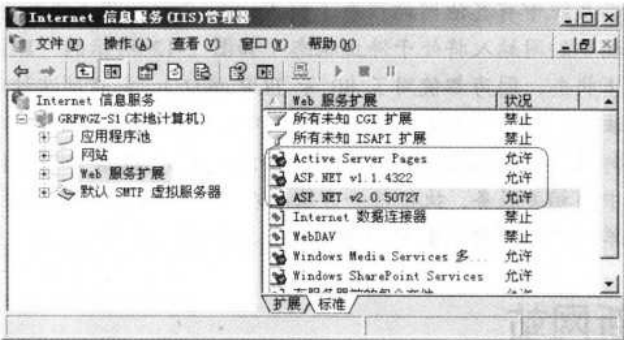


图 2-11 “Web 服务扩展”窗口

(2) 如果不是处于“允许”状态，可在相应选项上单击鼠标右键，在弹出的快捷菜单中选择“允许”命令启用这些扩展服务。

另外，如果在如图 2-9 所示的对话框中选择了“远程管理 (HTML)”选项，则会在 IIS 管理器控制台的“网站”容器下除了有一个“默认网站”外，还有一个用于通过互联网远程管理的 Web 网站的“Administration”网站；如果在如图 2-5 所示的对话框中选择“Windows SharePoint Services”和“Windows Media Services”这两个组件项，则会在“网站”节点下另外新增对应的 3 个站点（“Administrator”站点用于远程管理 Web 服务器；“SharePoint 管理中心”站点用来管理“SharePoint 服务”；而“Windows Media 管理站点”则是用来管理媒体站点的），如图 2-12 所示。否则只有一个“默认网站”，如图 2-13 所示。

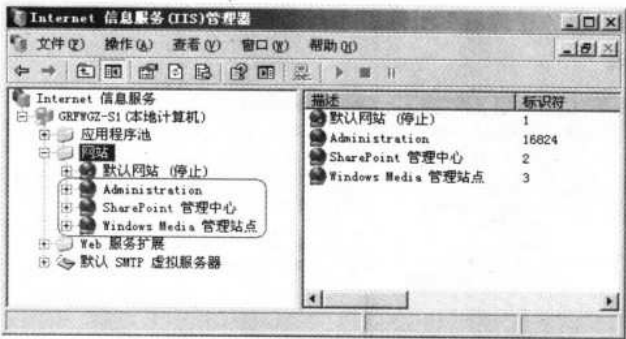


图 2-12 新增的 3 个站点的 IIS 管理器



图 2-13 只有一个默认网站的 IIS 管理器



注意

当系统中有其他网站程序（如 Apache Server 等）正在运行时，IIS 中使用相同端口的网站将处于停止状态（如图 2-12 所示的“默认网站”当前就处于停止状态，因为都使用了 80 号 TCP 端口）。要启动这种处于停止状态的网站方法有两种：一是更改所使用的端口，使各网站所使用的端口号不一致；另外是卸载其他网站程序（仅关闭程序没有用），或者关闭其他网站程序在服务窗口中的相关服务。执行任一方法后在相应网站上单击鼠标右键，在弹出的快捷菜单中选择【启动】命令即可重新启动停止的网站。

2.3 组建新网站

组建新 Web 站点的方法主要有两种：一是编辑系统默认提供的站点，适用于只需要一个网站的用户；另外是利用向导方式新建站点，适用于需要多个网站的用户。本节仅介绍向导方式，默认站点的编辑方式将介绍，它们的配置方法基本一样。

在 Windows 2000 Server /Server 2003 等服务器系统中都可以同时创建多个站点，而在 Windows 2000 Professional/XP 系统中却只能有一个站点，所以只能通过修改系统默认站点来配置新的站点。下面以创建一个名为“广州凌云计算机图书创作中心”网站为例进行介绍。具体的创建步骤如下。

(1) 在 IIS 管理器控制台的“网站”节点上单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【网站】命令，打开如图 2-14 所示向导对话框首页。

(2) 单击对话框中的【下一步】按钮，打开如图 2-15 所示的对话框。在“描述”文本框中输入站点的名称，在此输入“广州凌云计算机图书创作中心”。



图 2-14 “欢迎使用网站创建向导”对话框

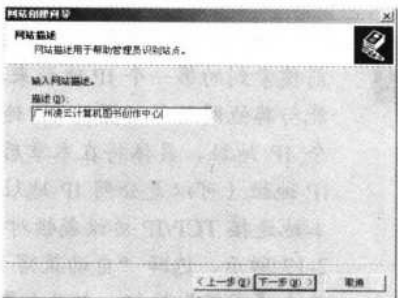


图 2-15 “网站描述”对话框

(3) 单击【下一步】按钮，打开如图 2-16 所示的对话框，在这个对话框中要求指定访问此站点的 IP 地址，TCP 端口（默认值为 80，最好不要改）、主机头值。“此网站的主机头”是指 Web 站点名最前面那部分主机名，实际上就是网站的域名，注意只是指合法的互联网域名。一个网站在网站属性对话框中可以配置多个主机头值，对应多个域名，但在此处只能输入一个主机头值，如笔者所申请有动态域名：lycbgz.xicp.cn。

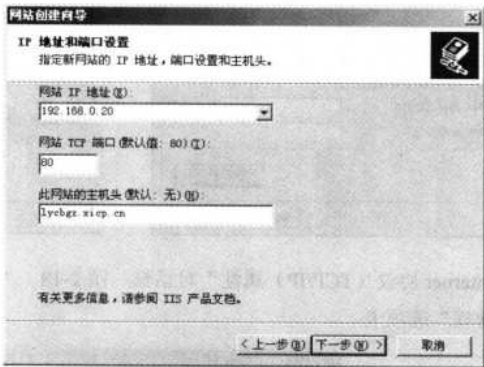


图 2-16 “IP 地址和端口设置”对话框

此处的 IP 地址配置最复杂，因为存在多种情况，而且不同情况的配置方式不一样。

如果 Web 网站仅用于局域网内部，则非常简单，仅需要在此“网站 IP 地址”下拉列表框中提供一个 Web 网站服务器局域网连接网卡上的一个 IP 地址即可。

如果 Web 网站是用于外网的，则要分情况而定了。如果 Web 服务器是直接连接互联网（不是通过共享方式上网的，不同共享上网方式的配置方法参见本系列丛书的《网管员必读——超级网管经验谈》一书），而且有固定公网 IP 地址（如各种专线连接方式），则在“网站 IP 地址”下拉列表框中指定唯一、静态的公用 IP 地址；如果是通过共享方式上网的，则在此“网站 IP 地址”下拉列表框中仍只能指定唯一、静态的局域网 IP 地址，外网固定 IP 地址指定在网关上（如路由器的 WAN 口，或者代理服务器的 WAN 网卡上）。

如果 Web 服务器虽然是直接连接互联网，但没有固定公网 IP 地址，而是采取像拨号上网之类的动态连接方式，此时就不能指定固定的 IP 地址了，则在“网站 IP 地址”列表框中

40 网管员必读——网络应用（第2版）

选择“全部未分配”选项即可。而如果在没有固定公网 IP 地址的同时，也不是直接连接互联网的，则需在“网站 IP 地址”列表框中为网站指定个服务器局域网连接网卡上的 IP 地址。



如果在以上各种情形下全部选择“全部未分配”选项，则系统会默认以当前搜索到的第一个 IP 地址来打开网站，此时如果 IIS 中部署了多个网站，则可能与其他网站所配置的 IP 地址相冲突，出现访问故障。一个网站可以配置多个 IP 地址，具体将在本章后面介绍。同时，一块网卡也可以配置有多个静态 IP 地址（可以是公网 IP 地址，也可以是局域网 IP 地址）。配置方法是在网卡本地连接 TCP/IP 协议属性对话框中选择“使用下面的 IP 地址”单选项（如图 2-17 所示，选择“自动获得 IP 地址”单选项时不能配置多个 IP 地址），然后单击【高级】按钮，打开如图 2-18 所示的对话框。在这里可在“IP 地址”栏中单击【添加】按钮，在打开的如图 2-19 所示的对话框中添加其他的 IP 地址。

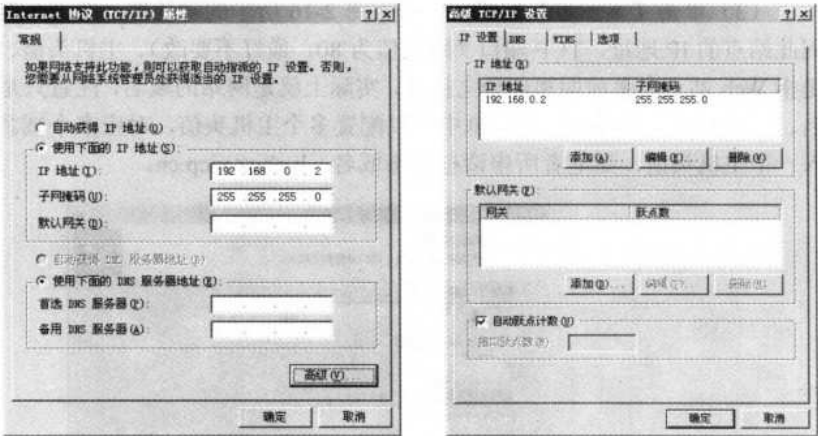


图 2-17 “Internet 协议（TCP/IP）属性”对话框 图 2-18 “高级 TCP/IP 设置”对话框
“常规”选项卡

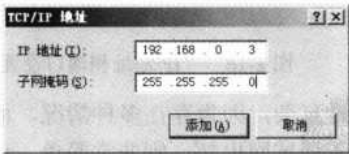


图 2-19 “TCP/IP 地址”对话框



网站的访问端口号系统默认为 80 号，不过当在同一服务器的同一块网卡中连接多个网站时，则一定要设置成不同的端口，否则会引起冲突，无法运行。不是采用默认的 80 号端口时，在访问时需要加上对应的端口号。如本示例中的网站计算机名为 lycbgz.xicp.cn，如果想把访问端口改为 8080，则用户在访问网站时需在浏览器地址栏中输入：http://lycbgz.xicp.cn:8080，后面那个“8080”就是访问端口。因为它不是系统默认的，不特别标明的话，系统仍会默认使用并未采用的 80 号端口，造成网站无法打开。

(4) 单击【下一步】按钮，打开如图 2-20 所示的对话框。在这个对话框中可以设置站点存放文件的主目录路径。这里的主目录可以是在本机上，也可以是网络的其他服务器上，但为了网站性能有足够的保证，建议把网站主目录设置在本地服务器上。

因为默认网站采用的是系统默认的 Inetpub\wwwroot 路径，新网站与它不一样了，但可以在 Inetpub 目录新建子目录，如 Inetpub\lycbgz，当然也可以是其他任意路径，不过一定要在 NTFS 格式磁盘分区下，因为这样可以为不同用户设置不同的访问权限。同时，在制作好了网站文件后一定要记得放在这个路径下。也不要与其他已有网站在同一目录下，以便于工作区别和管理。如果想让企业员工匿名访问或者外网用户访问该网站，则要选择“允许匿名访问此网站”复选项。如果选择了它，则用户登录时可不用输入账户和密码。匿名访问的权限最低，默认仅允许以“读取”方式访问，具体将在介绍网站配置时介绍。如果网站是企业内部网站，则最好不要允许以匿名方式访问，这样更加安全。

(5) 单击【下一步】按钮，打开如图 2-21 所示的对话框。在这个对话框中要为网站用户设置一个网站访问权限。为了确保站点的安全，对于普通用户，一般仅需选择“读取”权限项，其他权限可不选。对于特殊用户，可以通过配置不同用户的 NTFS 文件访问权限来实现，将在本章后面的网站安全配置中介绍。

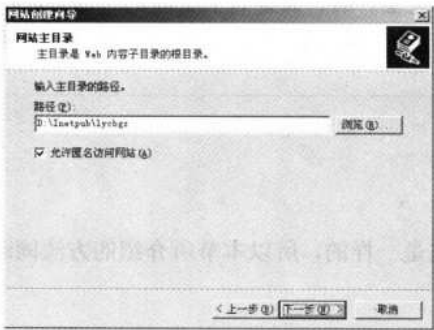


图 2-20 “网站主目录”对话框

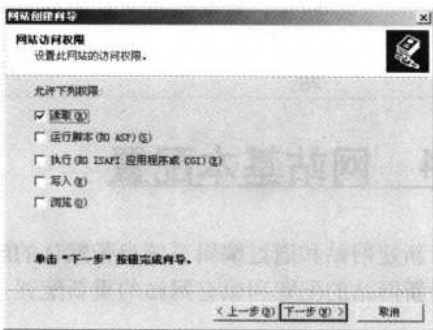


图 2-21 “网络访问权限”对话框

(6) 单击【下一步】按钮，打开如图 2-22 所示向导完成对话框。单击【完成】按钮即可完成一个新站点的整个创建过程，并返回到 IIS 主界面。此时在“网站”项中添加了刚才所创建的新网站，如图 2-23 所示。



图 2-22 “已成功完成网站创建向导”对话框

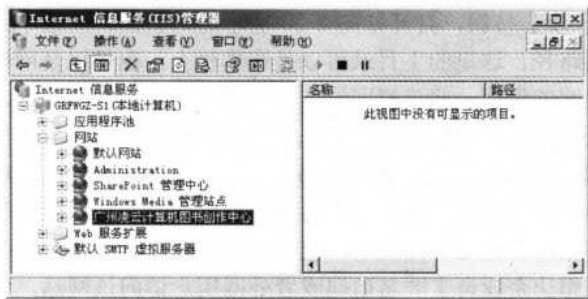


图 2-23 新建的网站窗口

新的网站创建后，如果事先没有把相应的网站文件搬到网站主目录下，则新网站是空的，如图 2-23 所示。此时可以通过其他方式（如 Dreamwear 和 FrontPage 等）配置的网站文件移到这个在如图 2-20 所示的对话框中指定的网站主目录下。



在网站下面还可以创建子网站，只需在相应网站上单击鼠标右键，在弹出的快捷菜单中选择【新建】下面的【网站】命令即可打开前面介绍的网站创建向导。创建的具体方法与上面介绍的完全一样，只是这里创建的子网站也有自己对应的主目录和主页文件，在访问时直接进入子网站，而不是直接进入父网站。

2.4 网站基本配置

新建网站和通过编辑系统自带默认的配置方法是一样的，所以本节所介绍的方法同时适用于新网站的配置和原有网站的重新配置。

2.4.1 网站基本信息配置

要访问一个网站，首先要确定的就是网站的名称、域名（相当于 URL，统一资源定位）IP 地址、端口号等。只有这些基本信息确定了，网站的成功访问才具备了前提条件。网站基本信息是在网站属性对话框“网站”选项卡中进行的。下面是具体的配置方法。

（1）在如图 2-23 所示 IIS 管理器窗口中选择要配置的网站（在此以选择上节新建的网站“广州凌云计算机图书创作中心”为例进行介绍），单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“网站”选项卡，如图 2-24 所示。

（2）在“网站标识”栏中的“描述”文本框中可以重新配置网站名称，但要注意它并不显示在打开的网站上，仅出现在 IIS 管理器的控制台树中，以便与其他网站区别。

在“IP 地址”下拉列表框中可以修改原来的 IP 地址指定（如服务器的连接和上网方式发生了改变），具体指派原则参见上节第（3）步介绍。

“TCP 端口”文本框是用来指派运行 Web 服务的 TCP 端口，默认值是端口 80。可以将端口更改成唯一的 TCP 端口号，但是如果更改端口号，则必须预先通知客户端以便请求该更改的端口号，否则它们的请求无法连接到服务器。端口号是必需的，该文本框不能为空。



图 2-24 网站属性对话框的“网站”选项卡

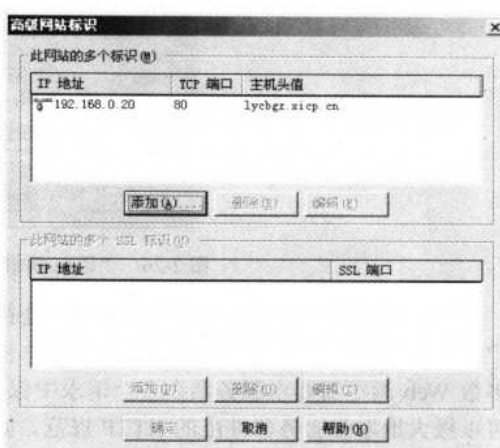


图 2-25 “高级网站标识”对话框

“SSL 端口”文本框是用来指派与该网站标识相关联的 SSL 端口。默认 SSL 端口号是 443。可以将 SSL 端口更改成任何唯一的 TCP 端口号，但要连接到服务器，则必须预先通知客户端以便请求该更改的端口号。只有使用 SSL 加密时才需要 SSL 端口号。如果没有为站点启用 SSL 加密，则“SSL 端口”文本框不可用。一般对外的网站不需要启用 SSL 加密，也就无须配置 SSL 端口号了。

(3) 单击【高级】按钮，打开如图 2-25 所示的对话框。在这里可以为网站配置多个标识。网站的标识有几种方法，可以仅通过 IP 地址进行，为每个网站分配一个或多个固定的 IP 地址（当然如果要把网站放在互联网上，则必须是唯一、固定的公网 IP 地址；如果网站服务器是共享上网的，或者网站仅用于局域网，则可以是唯一、固定的局域网 IP 地址）。也可以通过为不同的网站指定不同的服务端口，默认都是 80，如 Windows Server 2003 R2 IIS 自带的 Windows SharePoint Services 和 Windows Media Services 网站所用的端口分别为“8474”和“8080”，而自带安装的用于远程管理的 Administrator 网站，采用的端口为“8099”（此为普通访问时所用的 TCP 端口，安全访问（如服务器管理）必须为 8098 号 SSL 端口）；还可以通过主机头来标识，也就是域名，一个网站可以对应几个主机头值，如在不同域名服务商申请的多个域名。

在这里添加新的标识时一定要注意，新添加的标识在以上三项中至少要有一项是不一样的，当然也可以两项，甚至三项全部不同。

添加的方法是在如图 2-25 所示的对话框“此网站的多个标识”栏中单击【添加】按钮，打开如图 2-26 所示的对话框。按照前面介绍的原则配置对话框中的各项如果网站需要对外，则端口号最好不要改，仍为通用的 80，否则用户因不习惯，或者不知道使用方法而无法访问网站，因为改了端口号，访问时需要在域名后面加上“:端口号”，如现把端口改为 8080，则在访问 lycbgz.xicp.cn 时就需要以下：http://lycbgz.xicp.cn:8080 格式在浏览器地址栏中输入要访问的网站地址，而不能直接输入 http://lycbgz.xicp.cn。

这样配置了多个网站标识后，特别是配置了多个主机头值后，用户只要在地址栏中输入了已添加的主机头值，就可以访问到这个 Web 网站了。这就像一个公司有多域名，而网站内容却完全相同一样。

44 网管员必读——网络应用（第2版）

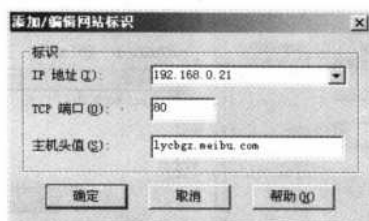


图 2-26 “添加/编辑网站标识”对话框

(4) 在如图 2-24 所示的对话框中的“连接”栏可以以秒为单位设置服务器断开不活动用户连接之前的时间长短。这将确保在 HTTP 协议无法关闭某个连接时，关闭所有的连接。大多数 Web 浏览器要求服务器在多个请求中保持连接打开，这称为“保持 HTTP 连接”。它是可以极大地增强服务器性能的 HTTP 规范。如果没有选择“保持 HTTP 连接”复选项，浏览器将不得不为包含多个元素（如图形）的界面进行大量的连接请求，可能需要为每个元素进行单独连接。这些额外的请求和连接要求额外的服务器活动和资源，这将会降低服务器的效率。其他请求特别是通过高滞后（慢）连接的请求，也可以使浏览器变慢并且响应变少。

在安装过程中，将默认启用“保持 HTTP 连接”复选项。其中的“连接超时”文本框中就可以键入数字（以秒为单位）设置服务器在断开与非活动用户的连接之前等待的时间（默认为 120 秒）。这将确保在 HTTP 协议无法关闭某个连接时，关闭所有的连接。而选择“保持 HTTP 连接”复选项可以使客户端与服务器保持打开连接，而不是根据每个新请求重新打开客户端连接。禁用“保持 HTTP 连接”可能降低服务器性能。默认情况下启用“保持 HTTP 连接”复选项。

(5) 继续在如图 2-24 中设置。如果在如图 2-24 所示的对话框中选择了“启用日志记录”复选项，则可以启用网站的日志记录功能，它可以记录关于用户活动的细节并按所选格式创建日志。信息存储在 ASCII 文件或 ODBC 兼容的数据库中。IIS 中的日志记录信息超出了常见的 Windows 系统事件日志或性能监视器功能的范围。日志包括的信息诸如：哪些用户访问了你的站点、访问者查看了什么内容，以及最后一次查看该信息的时间。可以使用日志来评估内容受欢迎程度或识别信息瓶颈。

在对话框中的“活动日志格式”下拉列表框中提供以下几种日志文件格式。

- Microsoft IIS 日志文件格式：一种固定的 ASCII 格式。
- NCSA 共用日志文件格式：一种固定的 ASCII 格式。
- ODBC 日志记录：一种记录到数据库的固定格式，与该数据库兼容。
- W3C 扩展日志文件格式：一种可自定义的 ASCII 格式，默认情况下选择此格式。

要使用进程记账，必须选择 W3SVC 扩展日志文件格式。

单击右边的【属性】按钮，打开如图 2-27 所示的对话框。在其中可以配置创建新日志文件的计划（例如，每小时、每天、每周、每月或按文件大小等），还可配置日志文件存储的目录位置。系统默认选择是每天新建一个日志文件。

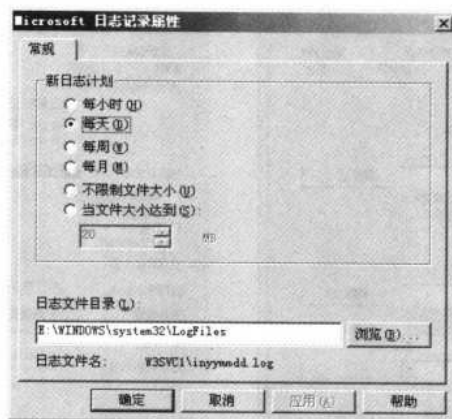


图 2-27 “Microsoft 日志记录属性”对话框

以上就是网站的基本信息配置。接下来要为网站指定主目录和主页文件。

2.4.2 为网站指定主目录和主页文件

网站主目录是用来存放网站文件的，就是把网站上的所有文件放在一个目录下；而网站主页文件是打开网站时默认打开的网页文件。

1. 网站主目录配置

网站主目录的配置涉及到网站属性对话框中的“主目录”选项卡，如图 2-28 所示。

在如图 2-28 所示的对话框中可以为网站指定一个存放所有网站文件的主目录，当然在这个主目录下可以任意创建子目录。通常 Web 服务器的主目录都位于本地磁盘系统，所以通常需选择“此计算机上的目录”单选项；如果是在网络的其他计算机上，则需选择“另一台计算机上的共享”单选项；如果是互联网上的某台服务器上，则还可以选择“重定向到 URL”单选项。在此以主目录在本地计算机上为例进行介绍。

如果选择“此计算机上的目录”单选项，则可直接在“本地路径”栏中输入主目录的地址（参见图 2-28），也可通过单击【浏览】按钮搜索。系统默认的网站主目录是在系统盘的 Inetpub\wwwroot 路径下，注意在配置网站文件时一定要把网页文件和子文件夹都放在这个目录中；当然如果选择的是其他目录作为网站主目录，则网站文件需存放在相应的目录下。

如果选择的是“另一台计算机上的共享”单选项，则图 2-28 所示的对话框将变为如图 2-29 所示，原来的“本地路径”栏变成了“网络目录”。在这里可以输入网站文件所在网络上其他计算机上的计算机名和共享名。格式为“\\服务器\共享名”，这就表明存放在网络中其他服务器上的网站主目录必须事先设置好共享属性。

同时，原来在如图 2-28 所示的对话框中的【浏览】按钮变成了【连接为】按钮，单击它，会打开一个名为“网络目录安全凭据”的对话框，在其中可以配置用于远程连接的用户账户信息。如果在其中选择了“在验证到网络目录的访问时总是使用已经过身份验证的用户凭据”复选项，系统会根据当前登录的用户名和密码来验证试图连接到远程共享的连接。清除该选项之后，所有到远程共享的客户端连接都将使用在上面配置的特定用户名和密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

46 网管员必读——网络应用（第2版）

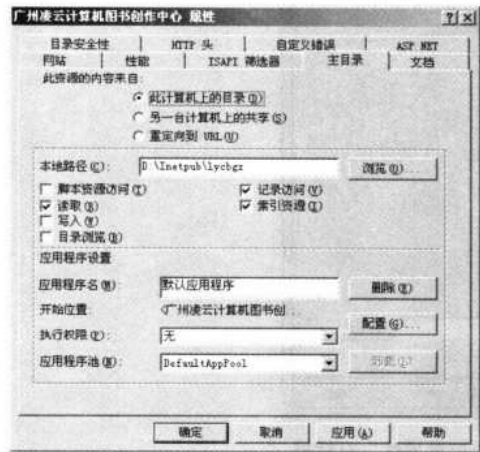


图 2-28 网站属性对话框“主目录”选项卡

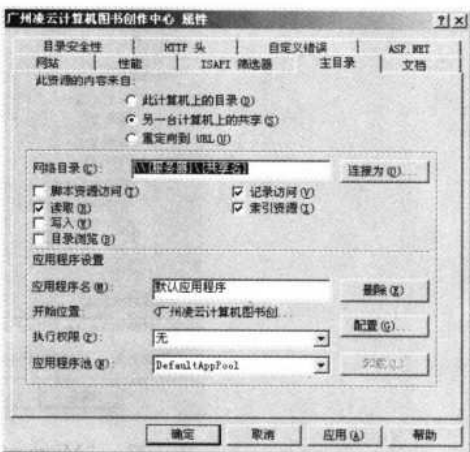


图 2-29 网站主目录在其他计算机上的“主目录”选项卡

如果所设的网站主目录是在其他网站（其实就是盗链）或虚拟目录上，此时需要在如图 2-28 所示的对话框中选择“重定向到 URL”单选项，此时对话框变成如图 2-30 所示。直接在“重定向到”文本框中输入要重定向的网站 URL 地址即可。

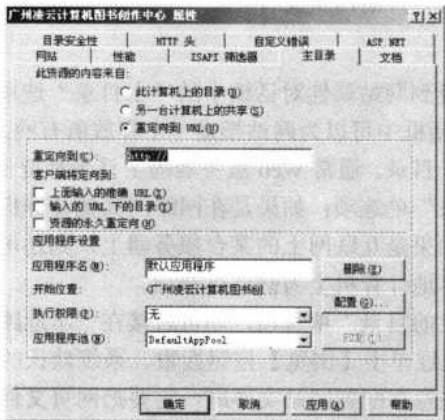


图 2-30 网站主目录为其他网站时的“主目录”选项卡

对比图 2-28、图 2-29 和图 2-30 3 个对话框可以看出，在如图 2-30 所示的对话框中，除了“此资源的内容来自”栏下的一个选项不同外，中间部分的其他选项也与这两个对话框不同。这是对用户访问网站的权限进行配置的。在这 3 个对话框中可以设置本地或网络路径以允许请求重定向到正确的物理位置。通过设置用户访问权限，选择是否记录对这些资源的请求，以及选择是否使用索引服务索引该站点，可以进一步配置物理位置。要指定何时接收请求，必须对应用程序进行标识、定位并给予适当的执行权限和保护。

在如图 2-28 和图 2-29 所示的两个对话框中，如果选择了“脚本资源访问”复选项，则当设置了读取或写入权限时，可以允许用户访问源代码。源代码包含 ASP 应用程序中的脚本。

如果选择“读取”复选项，则可以允许用户读取或者下载文件或目录及其相关属性。

如果选择“写入”权限项，则可以允许用户将文件及其相关属性上传到服务器上已启用的目录中，或者更改可写文件的内容。只有支持 HTTP 1.1 以上的版本协议标准 PUT 特性的浏览器，才允许具有写入权限。

如果选择“目录浏览”复选项，则可以允许用户看到该虚拟目录中的文件和子目录的超文本列表。因为虚拟目录不会出现在目录列表中，所以用户必须知道虚拟目录的别名。如果禁用了目录浏览并且用户未指定文件名，那么 Web 服务器将在用户的 Web 浏览器中显示“禁止访问”错误消息。

如果选择“记录访问”复选项，则可以将 IIS 配置成在日志文件中记录对此目录的访问。只有启用了该网站的日志记录之后，才会记录访问。

如果选择了“索引资源”复选项，则可以允许 Microsoft 索引服务将此目录包含到网站的全文索引中。

以上各选项，通常只需选择“读取”、“记录访问”和“索引资源”3个复选项。

在如图 2-30 所示的对话框中，如果选择了“上面输入的准确 URL”复选项，则可以将虚拟目录重定向到目标 URL，而不添加原始 URL 的任何其他部分。可以使用该选项将整个虚拟目录重定向到一个文件。例如，若要将对“/scripts”虚拟目录的所有请求都重定向到主目录中的 Default.htm 文件，可以在“重定向到”框中键入/Default.htm，然后选中该选项。

如果选择了“输入的 URL 下的目录”复选项，则可以将父目录重定向到子目录。例如，若要将主目录（由“/”符号指定）重定向到名为“/newhome”的子目录，可以在“重定向到”框中键入“/newhome”，然后选中该选项。如果不使用该选项，那么 Web 服务器会不断地将父目录映射到自身。

如果选择了“资源的永久重定向”复选项，则可以将下列消息发送到客户端：“301 永久重定向”。重定向被视为临时性的，并且客户端浏览器将接收到以下消息：“302 临时重定向”。某些浏览器可以使用“301 永久重定向”消息作为永久更改 URL 的信号（如书签）。

在如图 2-28、图 2-29 和图 2-30 所示的 3 个对话框中的“应用程序设置”栏中的选项是一样的。在“应用程序名”文本框中键入网站根目录的名称，该目录中包含了应用程序的文件和子目录。如果网站根目录采用的是系统默认的 Inetput\wwwroot 目录，则可直接按系统默认的“默认应用程序”设置。单击后面的【删除】（或【创建】按钮，单击一次【删除】按钮后即变为【创建】按钮），可以从网站删除或创建应用程序，同时保持虚拟目录不变。

在“开始位置”栏中显示的是上面在“应用程序名”文本框中配置的配置数据库节点，其实就是网站的描述。单击后面的【配置】按钮，打开如图 2-31 所示的对话框。在这里可以配置应用程序映射（也就是应用程序扩展名类型所对应的程序）、选项和调试功能。因为通常无须配置，所以在此也不多作介绍，以免复杂化。

在图 2-28、图 2-29 和图 2-30 所示的对话框中的“执行权限”下拉列表选项是用来确定该站点资源的许可的程序执行级别。具体可根据以下原则选择。

- 无：选择该选项可以限制只能访问静态文件，如 HTML 或图像文件。这是默认选择。
- 纯脚本：选择该选项可以只允许运行纯脚本，而不运行可执行程序。
- 脚本和可执行文件：选择该选项可以删除所有限制，以便所有文件类型均可以访问或执行。



图 2-31 “应用程序配置”对话框

在“应用程序池”下拉列表中显示的当前网站所使用应用程序池，可从下拉列表中选择可用的应用程序池。单击后面【卸载】按钮可以从内存卸载隔离的应用程序，或者卸载没有被其他应用程序引用的会集应用程序。

2. 网站主页文件配置

在如图 2-28、图 2-29 或者图 2-30 所示的对话框中单击选择“文档”选项卡，如图 2-32 所示，网站主页文件就是在这里配置的。在这个选项卡中一定要选择“启用默认文档”复选项，然后在下面的列表框中配置网站的主页文件名。启用后，只要浏览器请求没有指定文档名称，则将默认文档提供给浏览器。因为在 Web 站点中，其主页文件通常是以“Default.htm”、“Default.asp”和“index.htm”等这样的文件名来命名，所以在系统的默认设置中都把这几个文件名添加到默认文档列表中。如果自己的网站主页文件名没有在列表中，则要另外添加了。添加的方法很简单，只需单击【添加】按钮，打开如图 2-33 所示的对话框。在这里重新输入自己网站的主页文件名，然后单击【确定】按钮返回到如图 2-32 所示的对话框中即可。

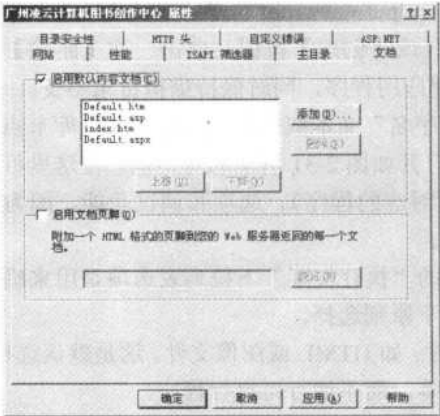


图 2-32 网站属性对话框“文档”选项卡



图 2-33 “添加内容页”对话框

默认文档可以是目录主页或包含站点文档目录列表的索引页。多个文档可以按照自上向下的搜索顺序列出。此处显示的文件一定要可在站点主目录中找到。使用【上移】和【下移】按钮可以修改顺序，通常是把自己网站当前使用的主页文件名排在最上面。



在站点打开时，首先要打开的是主页。在进行站点登录时，通常不用指定打开的文件名，而是直接在 IE 地址栏中输入站点的网址或域名。进入站点后首先打开的主页该如何定义呢？那就是在图 2-32 所示列表框中指定，系统是按自上向下的顺序来依次搜索执行的，即当在 Web 站点中搜索到符合第一个文档名的文件后，即自动启动这一文档，余下的文档将不再搜索，否则当站点中没搜索到符合文档列表中第一个文件名时，将继续搜索列表中符合第二个文档名的文件，搜索到则自动启动，否则继续向下搜索，以此类推。当列表中没有一个文件名与 Web 站点根目录中的文件名相符时，则显示无法访问的消息。

最好不要以“Default.htm”、“Default.asp”和“index.htm”之类的文件名来命名非主页文件。否则将启动一个非主页的 Web 端界面，不能正常使用 Web 站点了。

选择“启用文档页脚”复选项可以将 Web 服务器配置成自动附加页脚到 Web 服务器返回的所有文档中，不仅是网站主页文档，而且对于统一网站界面格式也非常有用。页脚文件就像 Word 文档中的页脚一样，通常用于标识一些诸如网站联系方式、地址、链接等网站信息。这样通过更改这里的文档页脚就可以随时更改网站下面的界面信息了。页脚文件不应该是完整的 HTML 文档，应该只包含格式化页脚内容的外观和功能时必要的 HTML 标记。单击【浏览】按钮可以查找和指定页脚文件的完整路径和文件名，它也必须是一个 HTML 网页文件。

2.5 网站安全及配置

如果要问 IIS 6.0 的主要改进是什么，那就是各种站点（特别是 Web 站点）的安全性有了明显的提高。在前些版本中，总有人怀疑，甚至直接地认为用 IIS 组建的网站安全性严重不足。这些在 IIS 6.0 版本中已得到极大地改善。

在 IIS 6.0 中，不仅在诸如身份验证、文件访问权限、数据加密和证书等常规安全措施方面提供了全方位的选择，而且还从底层提供了隔离模式选择，选择了工作进程隔离模式后，所有应用程序，就连与网站进程关系最密切的 HTTP 请求也被路由到正确的应用程序池队列中，这样一来所有应用进程都与系统底层服务完全隔离，从底层确保了系统的安全。本节就 IIS 6.0 Web 网站等各方面的安全性措施进行一一介绍，最后还将介绍各种安全措施的配置方法。当然，在实际的网络建设中，并不要求按本节后面介绍的方法进行全面配置，只需要有针对性地根据自己企业网络环境、网站的用途和应用需求选择一种，或少数几种进行配置即可。

2.5.1 IIS 6.0 的主要安全措施

IIS 6.0 中的一个最重要的变动涉及 Web 服务器安全性。Web 服务器计算机采取正确安

50 网管员必读——网络应用（第2版）

全措施，可以降低或消除来自怀有恶意的个人及意外获准访问限制信息或无意中更改重要文件的善意用户的各种安全威胁。这里仅简单地概述，具体安全措施的介绍将在本节后面相应小节进行。

1. 改进的核心功能和服务

对 IIS 6.0 已进行了重新设计以便利用基本 Windows 内核 HTTP.sys。这使其具有内置的响应和请求缓存和队列功能，并能够将应用程序进程请求直接路由到工作进程，从而改善可靠性和性能。

IIS 6.0 引入了两种用于配置应用程序环境的操作模式：工作进程隔离模式和 IIS 5.0 隔离模式。在安装 IIS 6.0 时默认的隔离模式取决于执行的是全新安装还是升级。

在全新安装 IIS 6.0 之后，IIS 以工作进程隔离模式运行。在从较低版本的 IIS 6.0 升级之后，隔离模式与以前安装的 IIS 6.0 版本所配置的相同。在从 IIS 5.0 或 IIS 4.0 升级之后，在默认情况下，IIS 6.0 以 IIS 5.0 隔离模式运行，这样可保持与现有应用程序的兼容性。

2. 安装锁定的 IIS

为确保 Windows 管理员不会因安装 IIS 而要处理不必要的安全威胁，IIS 6.0 安装时启用了静态网页请求处理功能，但禁用了所有其他请求处理功能。从安装 IIS 开始，IIS 6.0 的锁定安全配置文件可最大限度地减少入侵者的攻击面。IIS 6.0 安装和服务启用功能简化了与管理 IIS 服务有关的用于提高安全性的管理任务。仅当需要启用额外的服务时，才需要管理员进行进一步的干预。

当需要额外的服务时，Windows 管理员可通过 IIS 管理器中的 Web 服务扩展节点启用这些服务。当不再需要已启用的功能时，Windows 管理员可通过 IIS 管理器中的 Web 服务扩展节点禁用这些功能。

3. 身份验证

Internet 信息服务提供与 Windows 完全集成的安全功能。例如，IIS 支持以下 6 种身份验证方法。可以使用这些方法确认任何请求访问网站的用户的身份及授予访问站点公共区域的权限，同时又可防止未经授权的用户访问专用文件和目录。

- 匿名身份验证允许任意用户进行访问，不询问用户名和密码。
- 基本身份验证提示用户输入用户名和密码，然后通过网络“非加密”发送这些信息。
- 摘要式身份验证与“基本身份验证”非常类似，所不同的是将密码作为“哈希”值发送。摘要式身份验证仅用于 Windows 域控制器的域。
- 高级摘要式身份验证与“摘要式身份验证”基本相同，所不同的是“高级摘要式身份验证”将客户端凭据作为 MD5 哈希存储在运行 Windows Server 2003 的域控制器计算机上的 Active Directory 目录服务中，从而提高了安全性。
- 集成 Windows 身份验证使用哈希技术来标识用户，而不通过网络实际发送密码。
- 证书是可以用来建立安全套接字层（SSL）连接的数字凭据。它们也可以用于验证。

4. 访问控制

通过将 NTFS 访问权限用做 Web 服务器的安全基础，可以定义授予 Windows 用户和组文件和目录访问的级别。例如，如果一个企业决定在 Web 服务器上公布它的目录，则需要为企业创建一个 Windows 用户账户，然后配置特定网站、目录或文件的权限。权限应该只允许

服务器管理员和企业的所有人更新网站的内容；应该允许公共用户查看网站，但是不能更改网站的内容。要按此方式控制对目录和文件的访问，则必须使用 NTFS 格式的驱动器，而不能使用 FAT32 格式的驱动器。如果使用 FAT32，用户将拥有硬盘驱动器上每个文件的访问权限。

WebDAV 是 HTTP 1.1 协议的扩展，促进了基于 HTTP 连接的文件和目录管理。通过使用 WebDAV “动作”或命令，可以将属性添加到文件和目录中，以及从文件和目录中读取属性。文件和目录可以远程编辑、创建、删除、移动或复制。可以通过 Web 服务器权限或 NTFS 权限配置附加的访问控制。

5. 证书

证书是允许服务器和客户彼此验证的数字标识文档，通常只用于内网网站上，对于为外网用户提供的公共网站是不采用的。证书请求在服务器和客户端浏览器建立 SSL 连接，通过此连接可以发送加密信息。IIS 中基于证书的 SSL 特性由服务器证书、客户端证书和不同的数字密钥组成。可以使用 Microsoft 证书服务创建这些证书或者从可相互信任的第三方机构获得，该机构称为证书颁发机构（CA）。

服务器证书给用户提供了一种确认网站身份的方法。服务器证书包含详细的标识信息，如与服务器内容相关的机构的名称，签发证书机构的名称和用于建立加密连接的“公钥”。用户可使用此类信息确定 Web 服务器内容的真实性以及安全 HTTP 连接的完整性。

使用 SSL，Web 服务器还有通过检查客户端证书内容验证用户的选项。典型的客户端证书包含有关用户和签发证书及“公钥”机构的详细信息。可以使用客户端证书验证，结合 SSL 加密技术，实现安全性较高的方法以检验用户的身份。

6. 加密

可以允许用户以一种安全的方法（使用加密）与其服务器交换个人信息，如信用卡号或电话号码。信息在发送前由加密对其进行“编码”，接收后由解密进行“解码”。IIS 中的这种加密的基础是 SSL 3.0 协议，它提供了一种与用户建立加密通信链接的安全方法。SSL 确认网站的真实性同时可有选择地确认正在访问受限制网站用户的身份。

证书包括用于建立 SSL 安全连接的“密钥”。“密钥”是在建立 SSL 连接时验证服务器和客户端的唯一值。“公钥”和“私钥”组成 SSL “密钥对”。Web 服务器使用此密钥对与用户 Web 浏览器协商建立安全的连接，确定保护通信所需的加密级别。

对于此类型的连接，Web 服务器和用户浏览器都应该具有一致的加密、解密能力。在交换过程中，将创建加密密钥或“会话”密钥。服务器和 Web 浏览器都使用会话密钥加密、解密传输信息。会话密钥的加密程度或“强度”是使用“位”来测量的。最大的位号由会话密钥、加密和安全的最大级组成。尽管这些最大加密密钥强度提供了最大的安全性，但它们还是需要更多的服务器资源去实现。通常 Web 服务器的会话密钥长度为 40 位，但是根据所需的安全等级也可以是 128 位。

7. 服务器网关加密

服务器网关加密（SGC）使用 128 位加密为金融机构提供了全球金融交易解决方案。SGC 是安全套接字层（SSL）的扩展，它允许拥有 IIS 出口版本的金融机构可使用强加密。

SGC 不要求在客户浏览器上运行应用程序，并且可由 IIS 4.0 或更高版本的标准出口版本使用。为 SGC 配置的服务器可以增强 128 位和 40 位的加密会话，所以不要求多个 IIS 版本。

52 网管员必读——网络应用（第2版）

虽然 SGC 功能已内建到 IIS 4.0 及以后版本中，但是使用 SGC 时还需要特殊的 SGC 证书。

8. 可选的加密服务提供程序

通过使用可选的加密服务提供程序（CSP），可以选择 Microsoft 或第三方加密提供程序来处理加密和证书管理。每个加密提供程序可以创建一个公钥和私钥来加密发送到 Web 服务器和从中发送的数据。私钥存储在硬件的服务器端、PCI 卡、智能卡或者注册表中，这是因为它用于 Microsoft 安装的两个默认提供程序：Microsoft DH SChannel 加密提供程序和 Microsoft RSA SChannel 加密提供程序。每个提供程序的 Microsoft 加密 API（CryptoAPI）包含相同的方法和属性。因此，可以在提供程序之间切换，而无须重新编写代码。

9. 审核

可以使用安全审核技术监视大范围的用户和 Web 服务器的安全活动。推荐定期审核服务器配置，检测可能被未经授权访问影响和篡改资源的区域。可以使用集成的 Windows 实用程序、IIS 内置的日志记录功能或 Active Server Pages（ASP）应用程序创建自己的审核日志。

2.5.2 IIS 6.0 的应用程序隔离模式

在上节介绍到，IIS 6.0 的应用程序隔离模式可在两种不同操作模式下运行，它们分别是：工作进程隔离模式和 IIS 5.0 隔离模式。这两种模式都要依赖于 HTTP.sys 作为超文本传输协议（HTTP）侦听程序，然而，它们内部的工作原理是截然不同的。

工作进程隔离模式利用 IIS 6.0 的重新设计的体系结构并且使用工作进程的核心组件。IIS 5.0 隔离模式用于依赖 IIS 5.0 的特定功能和行为的应用程序。该隔离模式由 `IIsIsolationModeEnabled` 配置数据库属性指定。

所选择的 IIS 应用程序隔离模式对性能、可靠性、安全性和功能可用性都会产生影响。工作进程隔离模式是 IIS 6.0 操作的推荐模式，因为它为应用程序提供了更可靠的平台。工作进程隔离模式也提供了更高级别的安全性，因为运行在工作进程中的应用程序的默认标识为 `Network Service`。以 IIS 5.0 隔离模式运行的应用程序的默认标识为 `LocalSystem`，该标识允许访问并具有更改计算机上几乎所有资源的能力。

虽然工作进程隔离模式提供了增强的隔离性、可靠性、可用性和性能，但某些应用程序在以该模式运行时仍可能会有兼容性的问题。如果遇到了兼容性问题，请使用 IIS 5.0 隔离模式。当决定要使用哪种隔离模式时，请考虑以下情况。

- 除非由于特定的兼容性问题需要使用 IIS 5.0 隔离模式，否则使用工作进程隔离模式。
- 具有静态内容和简单的 Active Server Pages（ASP）应用程序的网站，在不修改或修改很少的情况下，应该能够以工作进程隔离模式运行。
- 如果应用程序能够在 IIS 5.0 上正确运行，它们就应该能够以 IIS 5.0 隔离模式正确运行。



IIS 6.0 无法同时运行两种应用程序隔离模式。因此，在同一台 IIS 服务器上，不可能以工作进程隔离模式运行某些 Web 应用程序，而以 IIS 5.0 隔离模式运行其他应用程序。如果有需要单独模式的应用程序，必须在单独的计算机上运行它们。

1. 工作进程隔离模式

工作进程隔离模式利用了所有新的 IIS 6.0 核心组件。使用工作进程隔离模式启用应用程序池、回收和运行状况检测功能，在本主题的后面将对这些功能进行描述。

如图 2-34 所示说明了以工作进程隔离模式运行的 IIS 6.0 体系结构。

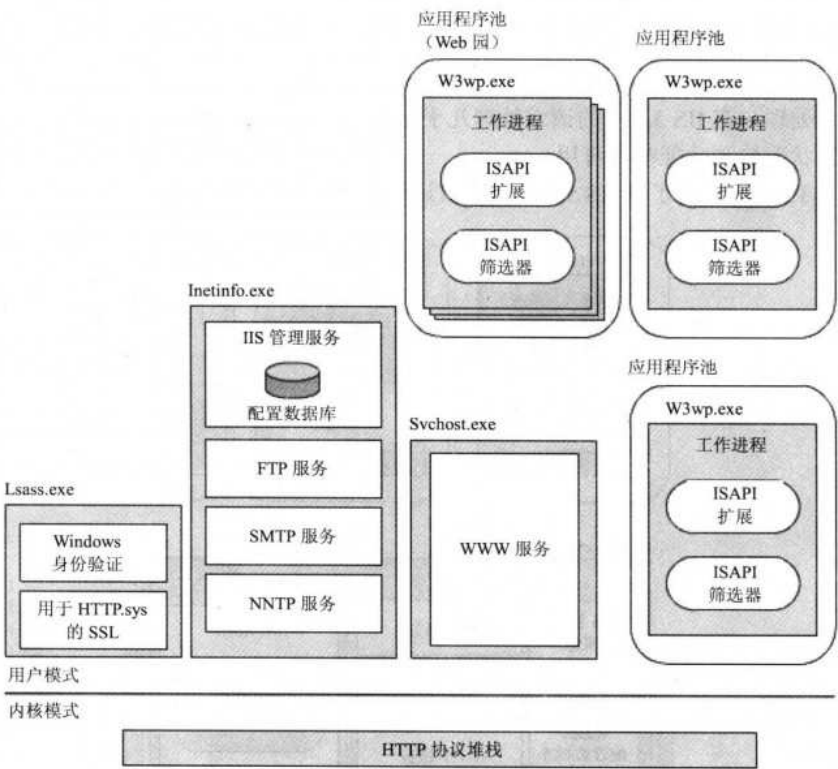


图 2-34 以工作进程隔离模式运行的 IIS 6.0 体系结构

在图 2-34 中可以看到，仅将应用程序特定代码加载到工作进程中。应用程序特定代码的示例是 ASP 和 ASP.NET 应用程序，因为这些编程平台的运行时引擎都是作为 Internet 服务器 API（ISAPI）扩展来实现的。

这种体系结构使得 IIS 非常可靠，因为不管在工作进程中发生了什么服务中断，万维网发布服务（WWW 服务）、IIS 管理服务和 HTTP.sys 都能不受其影响并且连续运行。同样，运行在工作进程中的网站也不受其运行在其他工作进程中的故障影响，因为它们通过进程边界彼此相互隔离。

下面的步骤说明了如何以工作进程隔离模式处理请求的。

- （1）请求到达 HTTP.sys。
- （2）HTTP.sys 确定请求是否有效。如果请求无效，它将向客户端返回一个无效的请求代码；如果请求有效，HTTP.sys 检查响应是否存在于其内核模式缓存中。
- （3）如果缓存中存在该响应，HTTP.sys 会立即返回该响应；如果没有缓存该响应，

- HTTP.sys 将确定正确的请求队列，并将此请求放在队列中。
- （4）如果没有为队列指派工作进程，HTTP.sys 将通知 WWW 服务启动一个工作进程。
 - （5）工作进程将该请求从队列中取出并对其进行处理。
 - （6）工作进程将响应返回给 HTTP.sys。
 - （7）HTTP.sys 将响应返回给客户端并记录该请求（如果做这样的配置的话）。

2. IIS 5.0 隔离模式

IIS 5.0 隔离模式确保为 IIS 5.0 而开发的应用程序的兼容性。以 IIS 5.0 隔离模式运行的 IIS 6.0 请求处理与在 IIS 5.0 下的请求处理几乎完全相同。在 IIS 5.0 隔离模式中，应用程序池、回收和运行状况检测功能都不可用。

如图 2-35 所示说明了以 IIS 5.0 隔离模式运行的 IIS。

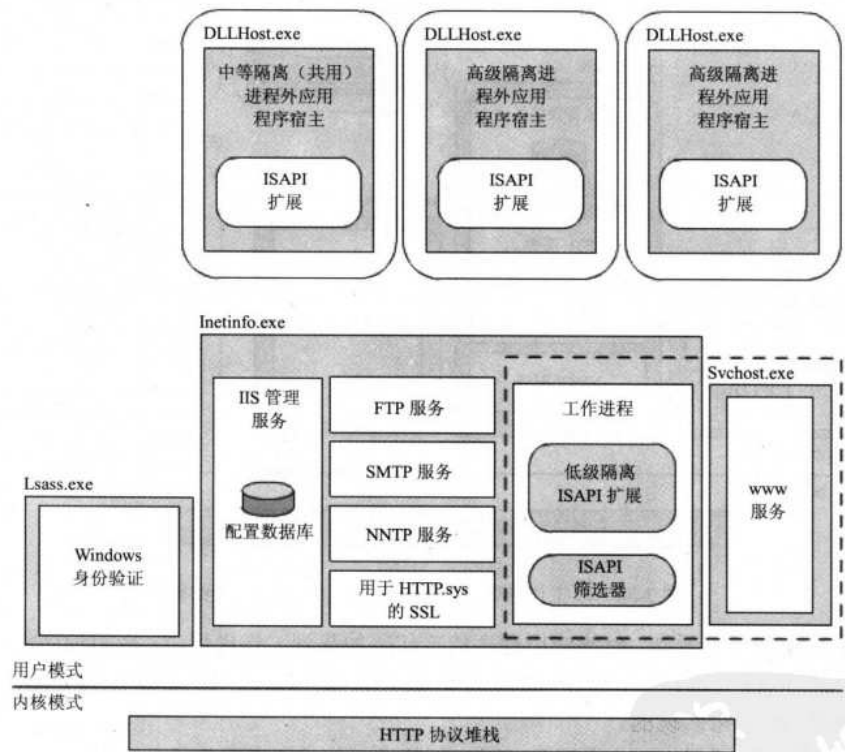


图 2-35 以 IIS 5.0 隔离模式运行的 IIS 6.0 体系结构

在 IIS 5.0 隔离模式中，HTTP.sys 以在工作进程隔离模式中相同的方式使用。唯一的例外是它仅把请求传递到由 WWW 服务维护的单个请求队列中。根据隔离模式的配置情况（在进程内、在池中或者在进程外）请求将会在 Inetinfo.exe 或 DLLHost.exe 中进行处理。

3. 比较 IIS 6.0 模式中的功能

为了便于理解，下面以列表的方式对 IIS 5.0 隔离模式和工作进程隔离模式中的 IIS 6.0 功能的角色进行横向比较，如表 2-4 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表 2-4 IIS 5.0 隔离模式和工作进程隔离模式功能比较

IIS 功能	IIS 5.0 隔离模式宿主/组件	工作进程隔离模式宿主/组件
工作进程管理	N/A	Svchost.exe/WWW 服务
工作进程	N/A	W3wp.exe/工作进程
运行进程内 ISAPI 扩展	Inetinfo.exe	W3wp.exe
运行进程外 ISAPI 扩展	DLLHost.exe	N/A（所有的 ISAPI 扩展都在进程内）
运行 ISAPI 筛选器	Inetinfo.exe	W3wp.exe
HTTP.sys 配置	Svchost.exe/WWW 服务	Svchost.exe/WWW 服务
HTTP 协议支持	Windows 内核/HTTP.sys	Windows 内核/HTTP.sys
IIS 配置数据库	Inetinfo.exe	Inetinfo.exe
FTP	Inetinfo.exe	Inetinfo.exe
NNTP	Inetinfo.exe	Inetinfo.exe
SMTP	Inetinfo.exe	Inetinfo.exe

4. 隔离模式默认值

当在一台没有安装早期版本 IIS 的计算机上安装 IIS 6.0 时，隔离模式会自动设置为工作进程隔离模式。如果从 IIS 的早期版本进行升级，隔离模式则会设置为 IIS 5.0 隔离模式。

表 2-5 指定了安装 IIS 6.0 时的默认隔离模式设置。

表 2-5 安装 IIS 6.0 时的默认隔离模式设置

安 装	隔 离 模 式
新安装 IIS 6.0	工作进程隔离模式
从 IIS 6.0 的早期版本进行升级	隔离模式没有改变
从 IIS 5.0 升级	IIS 5.0 隔离模式
从 IIS 4.0 升级	IIS 5.0 隔离模式

5. HTTP 筛选器

安全套接字层（SSL）请求是加密的，内核模式 HTTP 服务缺乏解密请求或对加密进行响应的能力。用户模式服务 HTTP 筛选器有效地解决了这个问题，该筛选器专门用来解密 SSL 请求并加密返回。HTTP 筛选器服务以两种 IIS 操作模式运行，如下所示。

- 当 IIS 6.0 以工作进程隔离模式运行时，Isass.exe 作为 HTTP 筛选器的宿主。
- 当 IIS 6.0 以 IIS 5.0 隔离模式运行时，Inetinfo.exe 作为 HTTP 筛选器的宿主。

2.5.3 隔离模式配置

工作进程隔离模式是 IIS 中的默认服务模式。工作进程隔离模式体现了 IIS 6.0 新结构的所有优点：可靠的应用程序池、自动重新启动、可扩展性、调试，以及精确的性能调整。Web 应用程序以“网络服务”标识运行，它具有以下安全性优点：与“本地系统”相比，“网络服务”账户具有较低的访问特权。建议用户使用工作进程隔离模式，除非必须运行与此模式冲突的应用程序。



要完成以下步骤，必须重新启动 IIS，这将暂时中断万维网发布服务(WWW 服务)。同时，必须是本地计算机上 Administrators 组的成员或者必须被授予了相应的权限才能执行下列步骤。作为安全性最佳操作，请使用不属于 Administrators 组的账户登录到计算机，然后使用运行方式命令以管理员身份运行 IIS 管理器。在命令提示符下，键入 runas /user:administrative_accountname “mmc%systemroot%\system32\inetmgr\iis.msc”，此时系统会提示输入管理员密码，如图 2-36 所示（此时所采用的是系统管理员账户 administrator）。

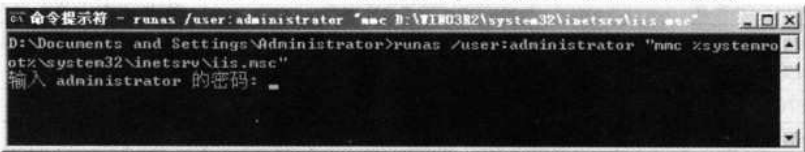


图 2-36 以系统管理员账户运行 IIS 管理器后的界面

正确输入密码后启动 IIS 管理器控制台。下面是具体的配置方法。

1. 将 IIS 配置为工作进程隔离模式

（1）在“IIS 管理器”控制台的“网站”选项上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“服务”选项卡，如图 2-37 所示。

（2）如果原来是以 IIS 5.0 隔离方式运行的，取消“以 IIS 5.0 隔离模式运行 WWW 服务”复选项的选择后会弹出如图 2-38 所示提示框。单击【是】按钮重新配置 IIS。

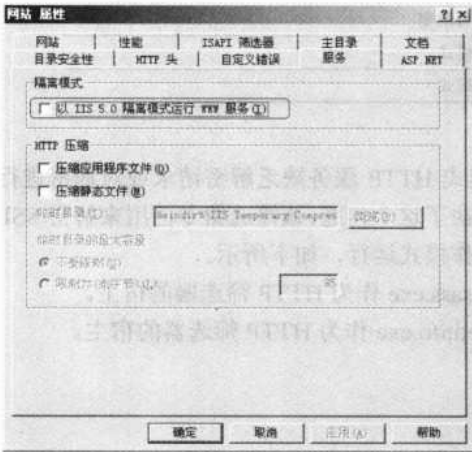


图 2-37 “网站属性”对话框“服务”选项卡

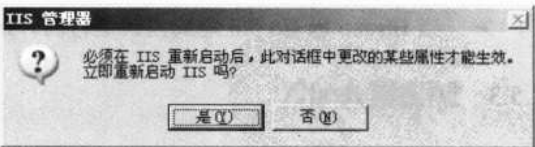


图 2-38 “IIS 管理器”提示框

如果成功切换到工作进程隔离模式，那么一个名为“应用程序池”的文件夹会出现在“IIS 管理器”的本地计算机列表中，如图 2-39 所示。可以如下方式来确定 IIS 当前运行的隔离模式：如果存在“应用程序池”文件夹，则为工作进程隔离模式；如果不存在“应用程序池”文件夹，则为 IIS 5.0 隔离模式。

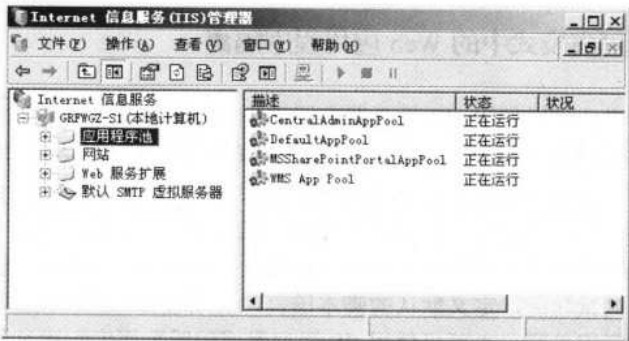


图 2-39 IIS 管理器中的“应用程序池”文件夹

2. 将 IIS 配置为 IIS 5.0 隔离模式

如果应用程序与工作进程隔离模式相冲突，则必须使用 IIS 5.0 隔离模式，直到该应用程序被修改。

以下的应用程序特性与工作进程隔离模式相冲突。

- 依存于 Inetinfo.exe: 如果应用程序必须在 Inetinfo.exe 进程中运行，则该应用程序必须在 IIS 5.0 隔离模式下运行，因为在工作进程隔离模式下应用程序不会运行在 Inetinfo.exe 中。
- 需要读取原始数据筛选器: 只有在 IIS 5.0 隔离模式中“读取原始数据”筛选器才可用。
- 需要 Dllhost.exe: 必须在 Dllhost.exe 环境中运行的应用程序只能在 IIS 5.0 隔离模式下运行，因为在工作进程隔离模式中 Dllhost.exe 不可用。

如果 IIS 6.0 服务正运行在工作进程隔离模式（IIS 6.0 的默认模式）下，而此时必须运行某些不能满足工作进程隔离模式要求的应用程序，则此时应该切换到 IIS 5.0 隔离模式。这意味着将不能利用工作进程隔离及该模式的其他功能。

配置成 IIS 5.0 隔离模式的方法就是在如图 2-37 所示的对话框中选择“以 IIS 5.0 隔离模式运行 WWW 服务”复选项。在应用配置时同样会弹出如图 2-38 所示提示框。重新启动 IIS 管理器后，则 IIS 管理器中原来的“应用程序池”文件夹不见了，如图 2-40 所示。

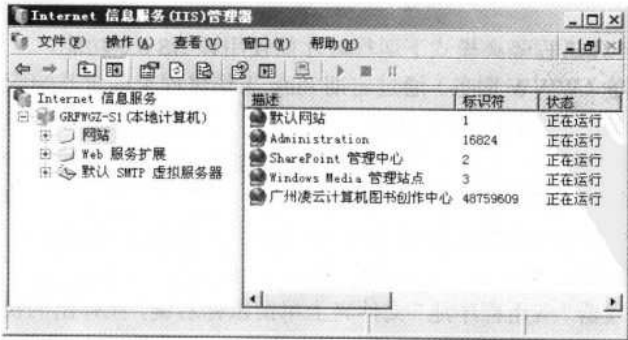


图 2-40 采用 IIS 5.0 隔离模式后 IIS 管理器中没有了“应用程序池”文件夹

2.5.4 工作进程隔离模式中的 Web 应用程序隔离

创建应用程序时，可以使用 IIS 管理器在网站中指定应用程序的开始位置目录（也称为应用程序根目录），每个网站可以有多个应用程序。安装 IIS 时所创建的默认网站是应用程序的开始位置。网站开始位置目录下的每个文件和目录均被认为是应用程序的一部分直至找到另一个开始位置目录。因此可以使用目录边界来定义应用程序的范围。

IIS 6.0 支持多种类型的应用程序及其配置选项。可以创建应用程序，然后对其进行配置以获得最佳性能和调试功能，定义默认的脚本语言，启用缓存、缓冲区及父路径，以及将文件扩展名与程序类型相关联。也可以使用 IIS 管理器或配置数据库配置这些选项。

IIS 6.0 中可能影响到当前 Active Server Pages (ASP) 应用程序的一项重要更改是默认情况下没有为 ASP 应用程序启用父路径。

理解了以上两种应用程序隔离模式后，本节和下节将分别具体介绍这两种隔离模式下的 Web 应用程序的隔离机制。应用程序隔离是指按进程边界来隔离应用程序，以防不同的应用程序互相影响。对于这两种 IIS 隔离模式，应用程序隔离的配置方式不同。本节先介绍工作进程隔离模式下的 Web 应用程序隔离原理和配置方法。

使用以工作进程隔离模式运行的 IIS 6.0，可以把 Web 应用程序分组编入“应用程序池”。应用程序池允许将特定配置设置应用于多个应用程序组，并允许工作进程为这些应用程序提供服务。可向应用程序池指派任何 Web 目录或虚拟目录。

应用程序池中的每个应用程序都共享相同的工作进程。因为每个工作进程都作为工作进程可执行文件 (W3wp.exe) 的单独实例操作，所以为应用程序池服务的工作进程之间是相互分离的。这就确保在 Web 应用程序发生故障时，它不会影响运行在其他应用程序池中的应用程序。可以配置和管理应用程序池来使用的功能包括：运行状况、工作进程回收、Web 园、处理器关系、应用程序池标识、IIS_WPG 组、预定义的账户和可配置的账户。

1. 应用程序池运行状况检测及配置

通过检测应用程序池的稳定（或运行状况）的程度，IIS 确定是否需要纠正操作。如果在指派到应用程序池的工作进程中所有可用的 IIS 线程都出现了阻塞，或者工作进程通知 IIS 存在故障，则万维网发布服务 (WWW 服务) 能检测到已经异常终止的不良运行状况的工作进程。

只有当 IIS 在工作进程隔离模式下运行时才能使用该 IIS 6.0 功能。

万维网发布服务 (WWW 服务) 通过定期 Ping 工作进程来确定其响应情况，监视工作进程的运行状况。如果工作进程没有对 Ping 作出响应，则 WWW 服务会终止该工作进程并创建另一个工作进程作为替换。此外，WWW 服务会保留每个工作进程的通信信道，并能够检测到通信信道的中断，这表示工作进程失败。如果工作进程由于其自身的原因失败，WWW 服务则将启动另一个工作进程取代它。

启动应用程序池运行状态监视的步骤如下。

(1) 在 IIS 管理器“应用程序池”文件夹上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“运行状况”选项卡，如图 2-41 所示。

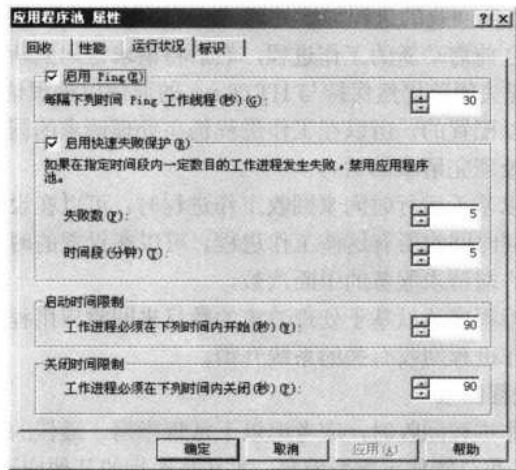


图 2-41 “应用程序池属性”对话框“运行状况”选项卡

(2) 选择“启用 Ping”复选项。在“每隔下列时间 Ping 工作线程”后面的“秒”滚动列表框中输入要在 Ping 之间相隔的秒数，默认为 30 秒。

(3) 单击【确定】按钮完成配置。

2. 工作进程回收及配置

工作进程回收是 Web 应用程序的自动刷新过程，它是通过重新启动指派给它们的工作进程来实现的。回收可使存在问题的应用程序保持顺利运行，尤其是在无法修改应用程序代码时。当发生回收事件时，当前正在处理应用程序池的工作进程就会终止，然后 WWW 服务会重新启动新的工作进程来替换它。

也只有当 IIS 在工作进程隔离模式下运行时才能使用这个 IIS 6.0 功能。

在工作进程隔离模式下，可以将 IIS 配置为定期重新启动工作进程，以便可以回收出错的 Web 应用程序。这可以确保这些池中的应用程序处于良好的运行状况并且可以确保系统资源能够恢复。

可以将工作进程配置为基于运行时间、处理请求的数目、计划的时间及两种内存使用类型来重新启动。

1) 工作进程回收如何工作

根据应用程序池回收的配置方式，万维网发布服务（WWW 服务）可以使用两种方法来回收已分配的工作进程：

- 在默认情况下，WWW 服务建立“重叠回收”，即继续运行要终止的工作进程，直到启动新的工作进程后为止。
- 或者，WWW 服务可以终止一个工作进程，然后启动一个新的工作进程（如果工作负荷允许执行此操作的话）。



注意

当 WWW 服务回收某个工作进程时，它并不断开现有的 TCP/IP 连接。HTTP 协议堆栈（HTTP.sys）建立并维护 TCP/IP 连接。

60 网管员必读——网络应用（第2版）

在重叠回收方案中，要回收的进程继续处理请求，同时 WWW 服务创建一个替代工作进程。在停止旧工作进程之前启动新的工作进程，然后将请求定向到新的进程。此设计可以防止服务中断，因为旧进程关闭前仍然保持与 HTTP.sys 的通信以处理请求。因为可重叠关闭或启动的关闭超时值是可以配置的，所以在工作进程仍在处理请求的同时可以终止该进程（如果它在时间限制内没有处理完请求的话）。

在配置应用程序池以基于运行时间来回收工作进程时，可以在设置的运行时间内回收所有的工作进程，但不能同时回收所有这些工作进程。可以在设置的时间内的不同时段进行回收应用程序，以减少客户端请求服务的中断次数。

类似的，在配置应用程序池以基于处理请求的数目来回收应用程序时，可以每隔一段时间回收一次以分担与工作进程回收有关的系统开销。

2) 何时使用工作进程回收

在决定是否启动工作进程回收时，应考虑以下常规指南。最佳的解决方案是修复引起故障的应用程序。但是，并非总能使用重新编码，尤其是运行的其他应用程序代码无法修改时。在以下情况下考虑使用回收。

- 无法修复 Web 服务器上所主控的有故障的应用程序。
- 遇到不能确定的或间断性的故障。
- 怀疑应用程序由于性能监视的原因而泄露内存。
- 先前已实施了临时性的重置解决方案，例如，计划执行 IISReset 命令行实用工具。

在以下情况下，可能根本不需要使用回收。

- 所主控的网站只包含静态内容，并且不包含自定义的 Internet 服务器 API (ISAPI) 应用程序。
- 所主控的应用程序已经过完全测试，并且不会出现内存或资源分配问题。

要有效地使用回收，请仔细检查回收所依据的项目，如表 2-6 所示。

表 2-6 使用回收时需要检查的项目

回收依据的条件	描 述	使用 时间
ISAPI 请求	根据应用程序池中 ISAPI 的请求回收工作进程	ISAPI 扩展可以将其自身声明为运行状况差
运行时间	根据用户指定的时间（分钟）回收工作进程	存在故障的应用程序的运行时间过长
请求数目	当超文本传输协议（HTTP）请求超出某个特定阈值时回收工作进程	根据应用程序接收到的请求数目，应用程序出现故障
计划的时间	在 24 小时内的指定时间进行回收	条件与运行时间的条件类似
虚拟内存（保留的内存加上已使用的内存）	当工作进程虚拟内存达到某个特定阈值时回收该工作进程	内存堆栈碎片过多（这是由于应用程序保留多次内存造成的）。症状是虚拟内存持续增加
已使用的内存	当 W3wp.exe 进程使用的内存达到某个特定阈值时回收工作进程	某些应用程序出现内存泄露
根据需要	当 IIS 管理员可以使用 Microsoft 管理控制台（MMC）或脚本控制整个应用程序池的回收时开始回收	在其他站点启动并运行时，有一个引起故障的应用程序池。请考虑回收该应用程序，而无须重置整个 WWW 服务

3) 回收工作进程的配置

根据需要可立即回收工作进程，配置的方法是在如图 2-41 所示的对话框中选择“回收”

选项卡，如图 2-42 所示。

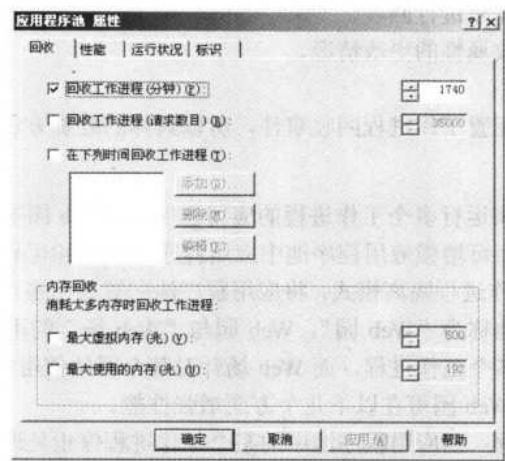


图 2-42 “应用程序池属性”对话框“回收”选项卡

配置要在经过一定时间后回收的工作进程，可在“回收”选项卡上，选中“回收工作进程（分钟）”复选项；在“回收工作进程（分钟）”右侧的滚动列表框中，键入在回收工作进程前的运行时间（分钟）。然后单击【确定】按钮完成配置。

配置要在处理一定数量的请求后回收的工作进程，则在“回收”选项卡上，选中“回收工作进程（请求数目）”复选项。在“回收工作进程（请求数目）”右侧的滚动列表框中，键入在回收工作进程前处理的请求数目。然后单击【确定】按钮完成配置。

配置要在计划的时间回收的工作进程，则在“回收”选项卡上，选中“在下列时间回收工作进程”复选项；单击【添加】、【删除】或【编辑】按钮，完成向列表中添加一个时间，删除一个时间或者更改现有的回收工作进程的时间。然后单击【确定】按钮完成配置。

注意 在将回收设置为在计划的时间进行时，如果修改了系统时间，则回收可能不在计划的时间进行。要避免无意中更改了回收时间，请在更改系统时间后，立即回收计划的工作进程。

配置要在消耗一定内存量之后回收工作进程，则在“回收”选项卡上，在“内存回收”下，选中“最大虚拟内存（兆）”复选项。在“最大虚拟内存（兆）”右侧的滚动列表框中，键入在回收工作进程前允许的最大虚拟内存数量；选中“最大使用的内存（兆）”复选项；在“最大使用的内存（兆）”右侧的滚动列表框中，键入在回收工作进程前允许的最大内存数量。最后单击【确定】按钮完成配置。

4) 记录工作进程回收事件

通过设置配置数据库属性 LogEventOnRecycle，可以使 WWW 服务在事件日志中记录工作进程回收事件。可以使用 LogEventOnRecycle 参数基于以下条件监视和记录回收事件。

- 所花的时间。
- 处理的请求。
- 计划的回收。

- 占用的内存。
- 根据管理员的需要进行回收。
- 应用程序池回收属性的更改情况。
- ISAPI 请求回收。

因一般情况下无须配置工作进程回收事件，所以具体的配置方法不再介绍。

3. Web 园及配置

Web 园是被配置用来运行多个工作进程的应用程序池。Web 园中的工作进程共享对特定应用程序池的请求，从而可增强应用程序池中应用程序的性能和可靠性。

可以使用 IIS 6.0 工作进程隔离模式，将应用程序池配置为由多个工作进程支持。使用多个工作进程的应用程序池称为“Web 园”。Web 园与“Web 场”的不同之处在于，Web 园针对某个应用程序池使用多个工作进程，而 Web 场针对某个网站使用多个服务器。

为应用程序池创建 Web 园可在以下几个方面增强性能。

- 可靠的请求处理：当应用程序池中的某个工作进程停止处理时（例如，当脚本引擎停止响应时），其他工作进程可以接受并处理该应用程序池的请求。
- 减少了资源争用：当 Web 园达到稳定状态时，按照循环方案每个新 TCP/IP 连接将分配给 Web 园中的一个工作进程。这可以产生平衡工作负荷和减少绑定到的工作进程的资源争用的效果。

只有当 IIS 在工作进程隔离模式下运行时才能使用这个 IIS 6.0 功能。

配置 Web 园的方法是在如图 2-42 所示的对话框中选择“性能”选项卡，如图 2-43 所示。在“Web 园”下的“最大工作进程数”滚动列表框中，键入要向应用程序池指定的工作进程数。然后单击【确定】按钮完成配置。

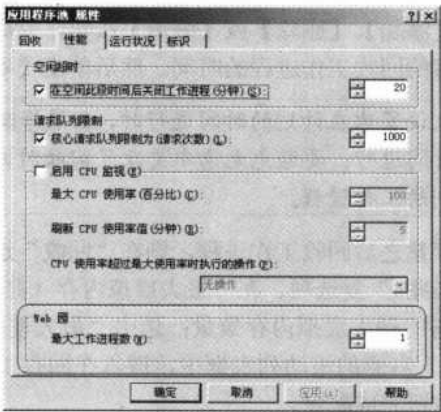


图 2-43 “应用程序池属性”对话框“性能”选项卡

4. 处理器关系

处理器关系是应用程序池的属性，该属性强制工作进程运行在特定的微处理器或 CPU 上，它应用于处理特定应用程序池的所有工作进程。使用了 Web 园和处理器关系的高级配置可用在多处处理器的计算机上，这样计算机中的 CPU 群集能专注于特定的应用程序池。通过将特定网络接口卡关系设置到特定 CPU 上，可以进一步地使用该配置。

在多 CPU 服务器上，可以配置应用程序池以便在工作进程和多个 CPU 之间建立关系，从而更有效地使用 CPU 缓存。可以结合使用处理器关系与处理器关联掩码设置来指定 CPU。只有当 IIS 在工作进程隔离模式下运行时才能使用这个 IIS 6.0 功能。

5. 应用程序池标识及配置

只有在工作进程隔离模式下运行时才能使用这个 IIS 6.0 功能。应用程序池标识是一种用户账户，应用程序池中的工作进程将使用该账户作为其进程标识。“进程标识”是操作系统术语，用来表示进程运行在其下的账户。每个运行在基于 Windows NT 操作系统上的进程都具有进程标识，用来控制对系统资源的访问。可以将预定义的账户或用户可配置的账户指派给应用程序池标识。

在默认情况下，应用程序池以“网络服务”账户身份来进行操作，该账户拥有低级别的用户访问权限。也就是说，该账户在攻击者或恶意用户可能试图控制正在运行万维网发布服务（WWW 服务）的计算机时，提供更好的安全性。“本地服务”账户同样具有低级别访问权限，该账户适用于那种不需要访问远程计算机资源的情形。你可以配置应用程序池以“本地系统”方式运行，本地系统是一个比网络服务或本地服务账户拥有更多用户权限的账户。但是，要注意在一个具有增强的用户权限的账户下运行应用程序池意味着较高的安全风险。例如，假设一个 Internet 服务提供商（ISP）要允许客户上载通用网关接口（CGI）应用程序并将其加入到应用程序池。以网络服务账户身份在应用程序池中运行启用 CGI 的应用程序，由于网络服务账户较低的用户权限，可以降低这些应用程序被用来攻击服务器的风险。

1) 选择标识

当选择应用程序池标识时，应选择具有应用程序所需要的最少特权的标识。如果编码如此，Internet 服务器 API（ISAPI）扩展会很容易地作为工作进程标识运行。在这种情况下，ISAPI 扩展所进行的操作都在工作进程标识的上下文环境中。当工作进程标识设置为具有高特权的账户（如本地系统）时，结果可能是应用程序被赋予了超出经过身份验证的用户范围的权限。因此，请考虑将工作进程标识设置为具有低特权的账户以防止 ISAPI 扩展以这种方式提高其特权。这样做可以防止应用程序破坏安全性。

2) 应用程序池标识与模拟用户的关系

模拟允许进程使用与其基本标识不同的安全凭据运行。因为两者通常容易混淆，理解由应用程序池标识创建的工作进程标识如何与模拟用户相关联是很重要的。

当 WWW 服务创建工作进程时，工作进程标识由与应用程序池标识相关的进程令牌创建。这样就建立了工作进程的进程标识。在默认情况下，工作进程所采取的所有操作都是在这个工作进程标识账户的上下文环境中完成的。然而，当处理客户端请求时，处理请求的线程在请求期间使用与该客户端相关的令牌，也就是经过身份验证的用户令牌，这也称为“模拟”。

应用程序中的行为如下所示：如果是匿名请求，经过身份验证的用户令牌与已配置的匿名用户相关（默认值为 IUSR_machinename 账户）；如果不是匿名请求，经过身份验证的用户的令牌则与用户的经过身份验证的账户相关。

在 IIS 处理 URL 之前，根据被请求资源的访问控制列表（ACL）来验证经过身份验证的用户令牌。另外，如果是对 ISAPI 扩展的请求（如 ASP），则工作进程将作为模拟令牌经过身份验证的用户令牌应用到调用 ISAPI 扩展的线程上。当 ISAPI 扩展开始处理请求时，模拟令牌应用到它所进行的操作上。因此，ISAPI 扩展所进行的操作与经过身份验证的用户相关，

64 网管员必读——网络应用（第2版）

而不是与进程标识相关。

3) IIS 6.0 标识和 IIS 5.0 标识

工作进程使用的进程标识与在 IIS 5.0 中使用的标识不同。这会影响已从 IIS 5.0 迁移而来，并期望进程标识作为特定的账户（如 IWAM_ComputerName）来运行的应用程序。同样，对于在 IIS 5.0 中创建的 Web 应用程序，标识由组件服务来配置；而在以工作进程隔离模式运行的 IIS 6.0 中，标识是在 IIS 管理器中配置的。

4) IIS_WPG 组

IIS_WPG 组是由 IIS 6.0 提供的用户组。IIS_WPG 组提供了 IIS 所需的最少特权集，并且，由于不必为标识手动指派特权，IIS_WPG 组为标识账户使用特定的用户提供了方便的方法。如果账户不在 IIS_WPG 组中且不具备相应的权限，则工作进程将无法启动。

5) 预定义的账户

预定义账户也称为“服务用户账户”，它由操作系统创建。IIS 允许用户为应用程序池标识选择的预定义账户包括：网络服务（NetworkService）、本地系统（LocalSystem）和本地服务（LocalService）。

在默认的情况下，这些账户都是 IIS_WPG 组成员，并且应用程序池标识设置为网络服务账户，该账户是这三个账户具有最低特权的账户。在配置账户及其生效前，建议将应用程序的安全要求与预定义账户的权限级别进行比较。

6) 可配置的账户

当使用该选项时，必须为应用程序池标识指定本地计算机或域用户名和密码。指定的账户应该是 IIS_WPG 用户组的成员。如果用户账户不在 IIS_WPG 组中，必须手动应用工作进程所需要的适当资源上的 ACL 设置，但不建议这样做。

要更改运行于应用程序池中的账户，需进行如下操作步骤。

（1）在 IIS 管理器控制台中，展开本地计算机，展开“应用程序池”文件夹，在相应应用程序池上单击鼠标右键（此时的配置仅适用于相应应用程序池，也可在“应用程序池”文件夹上单击鼠标右键，不过，此时的配置则适用于当前 IIS 管理器中所有的应用程序池），在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“标识”选项卡，如图 2-44 所示。

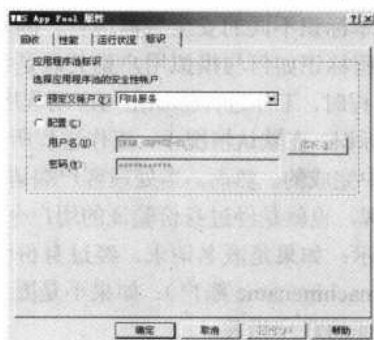


图 2-44 “应用程序池属性”对话框“标识”选项卡

（2）在“预定义账户”下拉列表框中选择标准的服务名选项，如“网络服务”（默认值）“本地系统”、“本地服务”。或者选择“配置”单选项，然后在下面配置已注册的用户名。

如果选择了“预定义账户”单选项，那么请在列表框中单击一个预定义的账户。如果选择了“配置”单选项，请在“用户名”和“密码”文本框中输入希望用来操作工作进程的账户的用户名和密码。然后，将该账户加入 IIS_WPG 组中。

(3) 单击【确定】按钮完成配置。

你可以隔离以不同标识运行在不同工作进程中的网站，但是，如果还希望使用 Kerberos 身份验证，那么会有一些限制。因为 Kerberos 需要某种服务支持，要使用 Kerberos 身份验证，某种服务必须注册其名称（称为服务主体名称（SPN）），以及运行该服务所使用的账户。在默认情况下，Active Directory 目录服务注册 NetBIOS 或者计算机名，并允许计算机账户使用 Kerberos。如果要以不同账户或使用不同名称（例如，如果计算机使用其他的 WINS 或 DNS 名）运行服务，那么可以使用 Setspn.exe 命令行工具设置 SPN。要设置 SPN，必须是域管理员。Setspn.exe 命令行实用程序可以在 Windows Server 2003 CD-ROM 内的支持工具包中获得。

如果使用集成 Windows 身份验证并且希望将本地用户账户或本地服务用做工作进程标识，那么不能使用 Kerberos 身份验证，因为 Active Directory 不信任这些账户。在这种情况下，必须强制 IIS 使用 NTLM 身份验证（也被称做 Windows NT 质询/响应验证）。

下面是使用 Setspn.exe 命令行实用程序的基本语法，其中“accountname”可以是单独的名称，也可以是域\名称。

Setspn [parameter] accountname

Setspn.exe 可使用表 2-7 所列的参数（parameter）。

表 2-7 Setspn.exe 可使用的参数

参 数	功 能	示 例
-R	重置 HOST ServicePrincipalName	Setspn -R computername
-A	添加任意的 SPN	Setspn -A SPN computername
-D	删除任意的 SPN	Setspn -D SPN computername
-L	列出已注册的 SPN	setspn -L SPN computername

下面的配置示例是使用 Setspn.exe 命令行实用程序注册以 Domain\UserAccount 运行的应用程序池的命令：

SETSPN.EXE -A HOST/<yourcomputername>Domain\UserAccount

下面的示例是注册 SPN “HOST/daserver1”和“HOST/{DNS of daserver1}”：

Setspn -R daserver1

下面的示例是计算机“daserver1”注册 SPN “http/daserver”：

Setspn -A http/deserver daserver1

下面的示例是从计算机“daserver1”删除 SPN “http/daserver”：

Setspn -D http/deserver daserver1

2.5.5 IIS 5.0 隔离模式中的 Web 应用程序隔离及配置

当以 IIS 5.0 隔离模式运行时，通过使用 AppIsolated 属性设置，可以为每个应用程序配置隔离。用于隔离的选项和运行 IIS 5.0 时一样，具体如下所示。

66 网管员必读——网络应用（第2版）

- 低（IIS 进程）：应用程序作为 `Inetinfo.exe` 中的 DLL 在进程内运行，并没有与其他运行于进程内的应用程序相互保护。默认的应用程序标识（应用程序运行的账户）是本地系统。
- 中（共用）：所有池中的应用程序都作为 `DLLHost.exe` 的一个实例中的 DLL 来运行且受到保护，以避免运行在低和高隔离中的应用程序的影响。然而，因为所有池中的应用程序都运行在相同进程中，它们相互之间没有受到保护。默认的应用程序标识是 `IWAM_ComputerName`。
- 高（独立）：应用程序都作为 `DLLHost.exe` 中的 DLL 来运行且受到保护，以避免受到其他应用程序的影响。同样，运行在同一台计算机上的所有其他应用程序也受到了保护，以避免受到运行在高隔离中应用程序的影响。默认的应用程序标识是 `IWAM_ComputerName`。

在安全考虑方面，当以 IIS 5.0 隔离模式运行 IIS 6.0 时，请设置为低隔离 Web 应用程序以本地系统标识运行。本地系统账户具有对计算机上所有资源的访问权，这意味着如果恶意用户的攻击成功地控制了被设置为低隔离的 Web 应用程序，则本地计算机上的所有资源都将暴露给攻击者。

设置为中或高隔离的 Web 应用程序以 `IWAM_ComputerName` 为默认标识来运行。

在性能考虑方面，当 IIS 以 IIS 5.0 隔离模式运行时，如果以高隔离配置运行应用程序就会有性能上的损失。这是由于公共对象模型（COM）使用了远程过程调用（RPC），这种情况就发生在下面的操作中。

- 当请求被发送到在高隔离下运行的应用程序且响应被发送回时。
- 在处理请求过程中，当在高隔离下运行的 Web 应用程序与 Web 服务器通信时。

与之相反，当 IIS 6.0 以工作进程隔离模式运行时，应用程序就会以进程内方式加载到 `W3wp.exe` 中，因此没有性能损失。

执行本节以下配置也必须是系统管理员或者授权的账户。

1. 隔离应用程序的配置

只有当 IIS 以 IIS 5.0 隔离模式运行时，才能使用该 IIS 6.0 功能。

“隔离”应用程序是指配置应用程序以使其与其他 Web 服务器和其他应用程序分隔的进程（内存空间）中运行。可以将应用程序配置为以上介绍的三种应用程序保护级别中的一种。请注意，在服务器端的包含文件（SSI）和 Internet 数据库连接器（IDC）应用程序无法在与 Web 服务器分隔的内存空间中运行。

要设置或更改应用程序保护级别，请执行以下步骤。

（1）在 IIS 管理器控制台中，展开本地计算机，在用于应用程序的网站或开始位置目录上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“主目录”、“虚拟目录”或“目录”选项卡（根据所选择对象不同而不同，在此以在网站上单击鼠标右键，选择“主目录”选项卡为例进行介绍）。如果位于被列为“开始位置”目录中，则“应用程序名”文本框已填好，如图 2-45 所示。



图 2-45 网站属性对话框“主目录”选项卡

- (2) 在“执行权限”下拉列表框中选择适当的保护级别。
- (3) 单击【确定】按钮完成配置。

2. 停止隔离的应用程序

同样，只有当 IIS 在 IIS 5.0 隔离模式下运行时才能使用这个 IIS 6.0 功能。
可以停止或从内存中卸载隔离的应用程序而无须停止 Web 服务器，这使测试和调试应用程序更加方便。
要停止和卸载隔离的应用程序，只需在如图 2-45 所示的对话框（同样有“主目录”、“虚拟目录”和“目录”3 种情况，图 2-45 只是其中一种情况）中单击【删除】按钮，然后单击【确定】按钮即可。如果【删除】按钮无效，则表明没有位于应用程序的开始位置目录。

2.5.6 匿名身份验证及配置

根据安全要求，可以选择一种 Internet 信息服务（IIS）验证方法对请求访问网站的用户进行验证。可以通过 IIS 管理器使用网站、目录或文件级别的属性页为 Web 资源设置验证方法。表 2-6 概述了网站验证方法。下面将分别介绍这些身份验证方式的工作原理和配置方法。这里介绍的是匿名身份验证及配置方法。

表 2-6 IIS 6.0 中可用的身份验证方法

方 法	安 全 级 别	如何发送密码	是否可以跨过代理服务器和防火墙使用	客户端要求
匿名身份验证	无	无	是	任何浏览器
基本身份验证	低	以 Base 64 编码的明文	是；但是因为以 Base 64 编码的明文没有进行加密，以明文方式通过代理服务器或防火墙发送密码存在安全隐患	大多数浏览器
摘要式身份验证	中等	哈希计算	是	IE 5.0 或更高版本
高级摘要式身份验证	中等	哈希计算	是	IE 5.0 或更高版本

(续表)				
方 法	安 全 级 别	如何发送密码	是否可以跨过代理服务器和防火墙使用	客户端要求
集成 Windows 身份验证	高	在使用 NTLM 时进行哈希计算；在使用 Kerberos 时应用 Kerberos 票据	否，除非在 PPTP 连接上使用	对于 NTLM，要求使用 IE 2.0 或更高版本；对于 Kerberos，要求使用带有 IE 5.0 或更高版本的 Windows 2000 或更高版本
证书身份验证	高	暂缺	是，使用 SSL 连接	IE 和 Netscape 浏览器
.NET Passport 身份验证	高	加密	是，使用 SSL 连接	IE 和 Netscape 浏览器

1. 匿名身份验证概述

匿名身份验证使用户无须输入用户名或密码便可以访问 Web 或 FTP 站点的公共区域。当用户试图连接到公共网站或 FTP 站点时，Web 服务器将连接分配给 Windows 用户账户 IUSR_computername，此处 computername 是运行 IIS 所在的计算机的名称。默认情况下，IUSR_computername 账户包含在 Windows 用户组 Guests 中。该组具有安全限制，由 NTFS 权限强制执行，它指出了访问级别和可用于公共用户的内容类型。

1) IUSR_computername 账户

下面是 IIS 使用 IUSR_computername 账户的基本原理。

- 在安装过程中，IIS 将 IUSR_computername 账户添加到运行 IIS 的计算机上的 Guests 组中。
- 在收到请求时，IIS 在运行任何代码之前先模拟 IUSR_computername 账户（IIS 可以模拟 IUSR_computername 账户，因为 IIS 知道该账户的用户名和密码）。
- 在将界面返回到客户端之前，IIS 检查 NTFS 文件和目录权限，查看是否允许 IUSR_computername 账户访问该文件。
- 如果允许访问，则访问进程（也称为“授权”）完成，并给用户这些资源；如果不允许访问，IIS 将尝试使用其他验证方法。如果没有作出任何选择，IIS 则向浏览器返回“HTTP 403 访问被拒绝”错误消息。



注意

如果启用了匿名验证，则 IIS 始终尝试先使用匿名验证对用户进行验证，即使启用了其他验证方法，也是如此。可以在 Web 服务器的服务级别，或单独虚拟目录和文件级别更改用于 IIS 管理器中匿名验证的账户，以启用其他需要的身份验证方式，允许其他高权限的用户进行更高级别的使用、维护和管理。

在 IIS 6.0 中，NETWORK_CLEARTEXT 是匿名验证的默认登录类型，采取这样登录类型的一种结果是匿名验证不再要求“允许本地登录”的用户权限。这样一来，即使用了 MMC 的组策略管理器管理单元来更改 Windows 中 IUSR_computername 账户的“允许本地登录”安全设置，以匿名验证方式的用户仍可以成功地在 Web 服务器上登录。但是，如果匿名用户账户不具有特定文件或资源的 NTFS 访问权限，Web 服务器仍将拒绝建立与该资源的匿名连接。

2) 子验证

在早期的 IIS 版本中，可以默认使用子验证组件 Iissuba.dll，该组件允许 IIS 管理匿名账户的密码。因为使用该组件有安全风险（因为密码可能被一些别有用心的人修改，造成其他

以匿名验证方式登录的用户不能成功访问），所以 IIS 6.0 不会默认启用子验证。但是，可以使用子验证管理匿名账户的密码，但必须满足以下条件。

- 对于授予匿名访问的应用程序，工作进程以 LocalSystem 身份运行。
- 注册了子验证组件 Iissuba.dll。
- 启用了 AnonymousPasswordSynch 配置数据库属性（设置为 TRUE）。

对于 IIS 6.0 全新安装和从配置了子验证的 IIS 安装升级到 IIS 6.0，为满足以上要求所采取的操作是不同的。

在全新安装后，IIS 6.0 默认在工作进程隔离模式下运行并禁用子验证（将 AnonymousPasswordSynch 设置为 FALSE）。启用子验证的机制如下。

- 通过打开命令提示并键入：rundll32 %windir%\system32\iissuba.dll,RegisterIISUBA 来注册 Iissuba.dll。
- 以 LocalSystem 身份使用匿名验证来运行所有工作进程。
- 将配置数据库属性 AnonymousPasswordSynch 设置为 TRUE。

在全新安装 IIS 6.0 后，如果切换到 IIS 5.0 隔离模式，则进程内应用程序分配的工作进程默认以 LocalSystem 身份运行。

在全新安装并切换到 IIS 5.0 隔离模式后配置子验证机制如下。

- 通过打开命令提示并键入：rundll32 %windir%\system32\iissuba.dll,RegisterIISUBA 来注册 Iissuba.dll。
- 将配置数据库属性 AnonymousPasswordSynch 设置为 TRUE。

在从使用子验证来管理匿名账户密码的旧版本 IIS 升级到 IIS 6.0 后，就会默认启用子验证（将 AnonymousPasswordSynch 设置为 TRUE），但子验证无法正常工作，因为有两项配置任务尚未完成。Iissuba.dll 没有注册，并且使用匿名验证的工作进程正在以 LocalSystem 身份运行。事件日志中应该有此类信息。

在从配置使用子验证的 IIS 安装升级到 IIS 6.0 后配置子验证机制如下。

- 通过打开命令提示并键入：rundll32 %windir%\system32\iissuba.dll,RegisterIISUBA 来注册 Iissuba.dll。
- 以 LocalSystem 身份使用匿名验证来运行所有工作进程。

2. 匿名身份验证配置

身份验证可以是针对网站、网站中的虚拟目录、目录和文件进行配置，它们的配置方法都是在对应的右键属性对话框中的“目录安全性”（配置网站或者虚拟目录时）或者“文件安全性”（配置文件时）选项卡中进行的。同时，它们之间又有继承和包含的关系，网站可以包括后面三者，而且都继承于网站的配置，所以一般情况在网站上进行的配置，将默认作用于虚拟目录、目录和文件。下面的身份验证方法和其他配置一样，不再另行说明。在此以具体的网站为例进行介绍。

（1）在 IIS 管理器控制台，选择要配置身份验证的网站，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“目录安全性”选项卡，如图 2-46 所示。

（2）在“身份验证和访问控制”栏中单击【编辑】按钮，打开如图 2-47 所示的对话框。

70 网管员必读——网络应用（第2版）

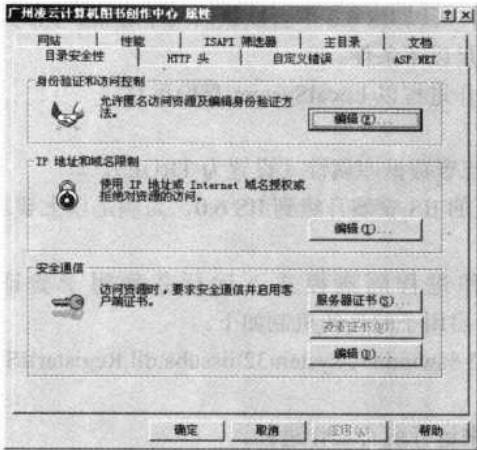


图 2-46 网站属性对话框“目录安全性”选项卡

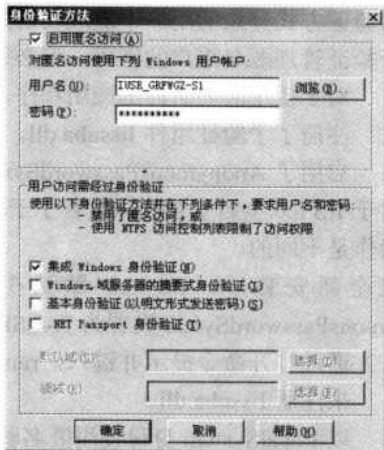


图 2-47 “身份验证方法”对话框

(3) 选中“启用匿名访问”复选项，然后在下面的“用户名”和“密码”文本框中依次键入要用于匿名访问的用户账户名和密码，默认的账户是 IUSR_computername 账户。也可通过单击【浏览】按钮，在打开的如图 2-48 所示的对话框中查找相应的用户账户。注意，此处只能选择用户账户，而不能选择组或计算机账户。

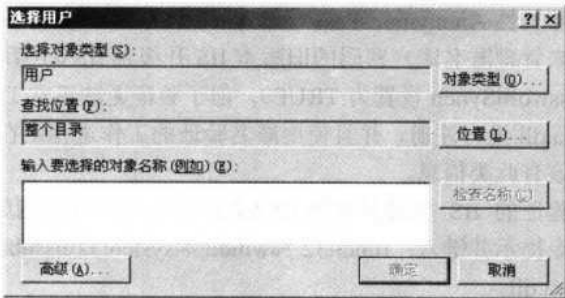


图 2-48 “选择用户”对话框

(4) 依次单击【确定】按钮返回到 IIS 管理器中即可完成匿名身份验证配置。

2.5.7 基本身份验证及配置

这种身份验证方式会提示用户输入用户名和密码，然后通过网络“非加密”发送这些信息。基本身份验证方法是广泛使用的工业标准方法，用于收集用户名和密码等信息。

1. 客户身份验证过程

以下步骤是 IIS 使用“基本身份验证”对客户端进行身份验证的基本原理。

(1) IE 浏览器显示一个对话框，如图 2-49 所示，以使用户输入先前分配的 Windows 账户用户名和密码（也称为“凭据”）。



图 2-49 采用基本身份验证方式登录网站打开时的身份验证对话框

(2) Web 浏览器试图使用用户凭据与服务器建立连接。在通过网络发送明文密码之前，该密码采用的是 Base 64 编码。



警告

Base 64 编码没有加密。如果使用 Base 64 编码的密码在网络中被网络嗅探器截获，则未经授权的用户可以很容易地对该密码进行解码并重新使用。

(3) 如果用户凭据被拒绝，则 IE 显示一个身份验证对话框，以重新输入用户凭据。IE 允许用户进行三次连接尝试，之后连接就会失败并向用户报告错误。

(4) 如果 Web 服务器证实用户名和密码与有效的 Windows 用户账户相符，则建立连接。

基本身份验证的优点在于它是 HTTP 规范的一部分，并且大多数浏览器均支持该验证。经过笔者实验，采用这种身份验证方式最容易配置成功。基本上是一次配置成功的。

这种身份验证方式的缺点是 Web 浏览器使用基本身份验证是以未加密的形式传输密码的。通过监视网络上的通信，攻击者或恶意用户可以使用常见工具很容易地截获和解码这些密码。因此，不建议使用基本身份验证，除非确信用户和 Web 服务器之间的连接是安全的，如专线或安全套接字层（SSL）连接。

2. 默认登录类型

在 IIS 6.0 中，基本身份验证的默认登录类型（配置数据库属性为 LogonMethod）也为 NETWORK_CLEARTEXT（它也适用于匿名身份验证）。这一点与旧版本 IIS 不同，旧版本的默认登录类型为 INTERACTIVE。正是由于这种变化，在使用基本身份验证的默认登录类型时，用户不再拥有 interactive 登录权限。基本身份验证适用于域控制器，而 NETWORK 和 NETWORK_CLEARTEXT 设置不再要求登录权限。有关基本身份验证所使用的登录类型的摘要如表 2-9 所示。

表 2-9 基本身份验证所使用的登录类型

登 录 类 型	LogonMethod（登录方式）设置	需要的登录权限	添加到访问令牌的安全标识符（SID）	是否需要出站凭据
NETWORK_CLEARTEXT T（默认值）	3-MD_LOGON _NETWORK_CLEARTEXT	网络	NTAUTHORITY \NETWORK_CLEARTEXT	是
NETWORK	2-MD_LOGON _NETWORK	网络	NTAUTHORITY \NETWORK	否

(续表)

登 录 类 型	LogonMethod (登录方式) 设置	需要的登录权限	添加到访问令牌的安全标识符 (SID)	是否需要出站凭据
BATCH	1-MD_LOGON _BATCH	批处理	NTAUTHORITY \BATCH	是

3. 令牌缓存安全注意事项

在使用基本身份验证时，将用户令牌缓存到令牌缓存中。在默认情况下，令牌在缓存中保留 15 分钟（以秒的形式表示）。如果使用基本身份验证及具有较高用户登录权限级别的账户登录，则攻击者一旦成功就可以使用该账户获得对计算机上资源的访问。可以使用以下几种方法来降低这种威胁。

- 不要使用基本身份验证及具有较高用户登录权限级别的账户登录，也不要允许任何用户以这种方式登录。
- 通过将全局注册表项 UserTokenTTL 设置为零，以将令牌缓存设置为不缓存用户令牌；或者将 UserTokenTTL 设置为小于默认值 15 分钟以将缓存的用户令牌设置为较短的保留时间。

4. 基本身份验证配置

它的配置方法与上节介绍的匿名身份验证方式类似，也是通过如图 2-46 和图 2-47 所示的两个对话框进行的。具体方法表现如下。

(1) 在如图 2-47 所示的对话框的“用户访问需经过身份验证”栏中选择“基本身份验证”复选项。由于基本身份验证通过网络发送未加密的密码，因此会出现一个警告提示框，询问是否希望继续。单击【是】按钮以继续。

(2) 在“默认域”（标识了用于用户身份验证控制的 Windows 域）文本框中键入要使用的域名，或者单击【选择】按钮以浏览新的默认登录域。如果已经填写了“默认域”文本框，则将该名称用做默认域。如果“默认域”文本框保留空白，则 IIS 将运行 IIS 的计算机的域用做默认域。IIS 配置 DefaultLogonDomain 属性的值，它决定了验证访问 IIS 服务器的客户（使用基本身份验证）所使用的默认域。但是，DefaultLogonDomain 属性指定的域仅用于客户在客户端计算机上出现的登录对话框中没有指定域的情况下。

(3) 此步可选。可以在“领域”文本框中键入一个值（可选），该框用于配置 Realm 属性的值。“领域”文本框标识了用于验证用户或组的域或其他操作系统身份验证控制器。如果设置了“领域”属性，那么当使用基本身份验证时，其值将出现在客户的登录对话框中。仅出于参考目的将“领域”属性值发送到客户，在使用基本身份验证时，不能使用该值对客户进行身份验证。

(4) 依次单击【确定】按钮两次完成配置。

2.5.8 摘要式身份验证及配置

与基本身份验证非常类似，所不同的是将密码作为加密后的哈希值发送。摘要式身份验证仅用于 Windows 域控制器的域。摘要式身份验证在通过网络发送用户凭据方面提高了安全性。摘要式身份验证将凭据作为 MD5 哈希，或消息摘要在网络上传送（无法从哈希中解密

原始的用户名和密码)。在 Web 分布式创作和版本控制 (WebDAV) 目录中可以使用摘要式身份验证。

1. 摘要式身份验证的要求

在运行 IIS 的服务器上启用高级摘要式身份验证之前，必须满足以下最低要求。

- 所有将访问使用高级摘要式身份验证保护的资源的客户端使用 IE 2.0 以上版本。
- 用户和运行 IIS 的服务器必须是相同域的成员，或者用户必须是可信域的成员。
- 用户必须将有效的 Windows 用户账户存储在域控制器上的 Active Directory 中。
- 域必须拥有运行 Windows Server 2003 家族成员的域控制器。如果域控制器位于运行 Windows 2000 的计算机上，则 IIS 6.0 需要使用子验证以使摘要式身份验证能够正常工作。
- 运行 IIS 的计算机必须安装了 Windows 2000 或更高版本。



注意

如果域控制器位于运行 Windows 2000 的计算机上，则 IIS 6.0 需要使用子验证以使摘要式身份验证能够正常工作。运行 IIS 的计算机必须安装了 Windows 2000 或更高版本。另外，如果服务器在工作进程隔离模式下运行，则必须以 LocalSystem 账户的身份运行。

2. 子验证

当域控制器运行 Windows 2000 时，要在 IIS 6.0 中使用摘要式身份验证，必须启动子验证（在 IIS 6.0 上没有默认安装）。要启用子验证，必须满足 3 个要求。

- 安装子验证组件 iissuba.dll。
- 将 UseDigestSSP 配置数据库属性设置为 FALSE。
- 将应用程序池的标识设置为 LocalSystem。

安装子验证组件的方法如下。

(1) 执行【开始】→【运行】菜单操作，在“运行”窗口中键入 cmd 命令，然后单击【确定】按钮进入命令提示符状态。

(2) 在命令提示符下键入：rundll32 systemroot\system32\iissuba.dll,RegisterIISUBA，然后按回车键。

(3) 对于任何使用摘要式身份验证的应用程序池，请将标识设置为 LocalSystem。

当不再需要使用子验证时，撤销注册子验证组件。撤销注册子验证组件的方法如下。

(1) 执行【开始】→【运行】菜单操作，在“运行”窗口中键入 cmd 命令，然后单击【确定】按钮进入命令提示符状态。

(2) 在命令提示符下键入：rundll32 systemroot\system32\iissuba.dll,UnregisterIISUBA 命令，然后按回车键即可。

3. 客户身份验证过程

以下步骤概述了如何使用摘要式身份验证对客户进行身份验证，如图 2-50 所示。

- (1) 客户从运行 IIS 的服务器请求文件。

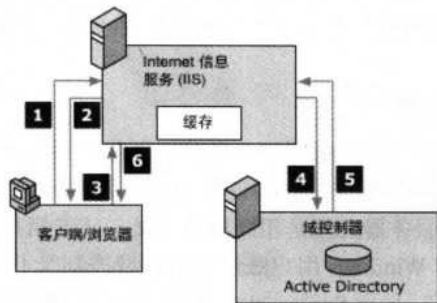


图 2-50 摘要式身份验证的客户身份验证过程

- (2) 运行 IIS 的服务器拒绝请求，并给客户端发送：正在使用摘要式身份验证和领域名称信息。
- (3) IE 浏览器提示用户输入凭据（用户名和密码），对话框参见图 2-49 所示。然后 IE 合并这些凭据和领域名称以创建一个 MD5 哈希，并从运行 IIS 的服务器中重新提交文件请求，此时发送的是 MD5 哈希。
- (4) 运行 IIS 的服务器接收哈希，并将客户端的哈希发送到域控制器以进行验证。
- (5) 域控制器向运行 IIS 的服务器通知验证结果。
- (6) 如果客户端已经过身份验证，则 IIS 将请求的文档或数据发送到客户端。



注意

仅当域控制器拥有 Active Directory 中存储的所请求用户密码的可逆加密（明文）副本时，摘要式身份验证才会完成。要以明文方式存储密码，如果仅针对特定用户，则可在 Active Directory 中激活用户“账户”选项卡上的“使用可逆的加密保存密码”设置，如图 2-51 所示；如果要针对域中所有用户，则可在域组策略中启用“用可还原的加密来存储密码”策略选项，以启用该功能，配置位置如图 2-52 所示。在指定此设置后，需要设置新的密码以激活此功能，因为无法确定旧密码。这一点要特别注意，因为如果不进行以上配置，在采用摘要身份验证方式时，就仍出现无法访问网站，最终显示无权访问的提示。



图 2-51 用户属性对话框“账户”选项卡



图 2-52 “组策略编辑器”窗口“密码策略”选项

4. 摘要式身份验证配置

摘要式身份验证方式的配置也是通过如图 2-46 和图 2-47 所示的对话框进行的。具体步骤如下。

(1) 在如图 2-47 所示的对话框的“用户访问需经过身份验证”栏中选择“Windows 域服务器的摘要式身份验证”复选项。

(2) 在“领域”文本框中键入领域的名称，或者单击【选择】按钮以浏览域。

可以在运行 IIS 的服务器上配置一个或多个领域名称。例如，给 domain1 的成员授予访问 sales 虚拟目录的权限，给 domain2 的成员授予访问 engineering 虚拟目录的权限。它尤其适用于 domain1 和 domain2 没有受信关系的情形。如果配置多个领域名称，则必须在不同的配置数据库级别中对它们进行配置。

如果没有给配置数据库中的某个子项配置领域名称，则该子项从配置了领域名称的上一个父项继承领域名称。如果没有配置领域名称，则 IIS 发送其自己的计算机名称作为领域名称。如果 IIS 发送其自己的名称作为领域名称，并且 IIS 不是在具有 Active Directory 的 Windows Server 2003 家族域控制器上运行，摘要式身份验证将失败。由于安全风险和性能方面的原因，建议不要在域控制器上运行 IIS（尽管也可以在上面运行）。

(3) 同样依次单击【确定】按钮两次完成配置。



注意 如果为所配置的站点、虚拟目录或文件夹启用了基本身份验证，则还可以使用“默认域”文本框。但是，对于摘要式身份验证而言，只有“领域”注意选项是有效的。

除了使用 IIS 管理器配置领域名称外，还可以使用脚本在任何配置数据库级别配置领域名称，如表 2-10 所示。如果没有特别配置子项，则它将从上一配置级别继承其配置。

表 2-10 可配置领域的配置数据库级别

配置数据库级别	描 述
W3SVC	W3SVC 级别（也称为 IISWebService 级别）是可以配置摘要式身份验证的配置数据库中的最高级别。没有具体配置设置的较低级别可以继承在此级别设置的配置
W3SVC/n	W3SVC/n 级别（也称为 IISWebService 级别）是特定的网站，其中 n 是该站点的编号。站点从 1 开始编号。默认网站为 1
W3SVC/n/root	W3SVC/n/Root 级别（称为 IISWebVirtualDir 级别）是网站的起点，其中 n 是该站点的编号
W3SVC/n/root/vdir	W3SVC/n/Root/WebVirtualDir 级别（称为 IISWebVirtualDir 级别）是网站中的虚拟目录，其中 n 是该站点的编号
W3SVC/n/root/vdir/webdir	W3SVC/n/Root/WebVirtualDir/WebDir 级别（也称为 IISWebDirectory 级别）是网站内虚拟目录中的物理目录，其中 n 是该站点的编号
W3SVC/n/root/vdir/file	W3SVC/n/root/vdir/file 级别是 W3SVC/n/Root/WebVirtualDir 级别中的单独文件，其中 n 是该站点的编号
W3SVC/n/root/vdir/webdir/file	W3SVC/n/root/vdir/file 级别是 W3SVC/n/Root/WebVirtualDir/WebDir 级别中的单独文件，其中 n 是该站点的编号

2.5.9 高级摘要式身份验证及配置

摘要式身份验证提供与基本身份验证相同的功能，但是，摘要式身份验证在通过网络发送用户凭据方面提高了安全性。摘要式身份验证将凭据作为 MD5 哈希或消息摘要在网络上传送（无法从哈希中解密原始的用户名和密码）。在 Web 分布式创作和版本控制（WebDAV）目录中可以使用摘要式身份验证。

不需要安装额外的客户端软件；但正如万维网联合会网站中的 RFC 2617 规范所定义的一样，摘要式身份验证依赖于 HTTP 1.1 协议。因为摘要式身份验证需要与 HTTP 1.1 兼容，所以并非所有的浏览器均支持该验证。如果与 HTTP 1.1 不兼容的浏览器从使用摘要式身份验证的服务器请求文件，则该服务器将要求客户端提供摘要式身份验证凭据。与 HTTP 1.1 不兼容的客户端拒绝该请求，因为客户端不支持摘要式身份验证。

1. 高级摘要式身份验证的要求

在运行 IIS 的服务器上启用高级摘要式身份验证之前，必须满足以下最低要求。只有域管理员才能够验证是否达到域控制器要求。如果不知道域控制器是否达到以下要求，请与域管理员联系。

- 所有将访问使用高级摘要式身份验证保护的资源的客户端使用 IE 5.0 或更高版本。
- 用户和运行 IIS 的服务器必须是相同域的成员，或者用户必须是可信域的成员。
- 用户必须将有效的 Windows 用户账户存储在域控制器上的 Active Directory 中。
- 域必须拥有运行 Windows Server 2003 家族成员的域控制器。
- 域控制器和运行 IIS 的服务器必须均运行 Windows Server 2003 家族的成员或更高版本。如果域控制器或 IIS 服务器运行 Windows 2000 或更低版本，则 IIS 默认使用摘要式身份验证，并且不会警告此操作。

2. 高级摘要式身份验证的客户端验证过程

高级摘要式身份验证的客户端验证过程如下。

如图 2-53 所示显示如何使用高级摘要式身份验证对客户端进行身份验证的过程，用文字描述如下（以下各步对应图中的序列号）。

- (1) 客户端从运行 IIS 的服务器请求文件。
- (2) 运行 IIS 的服务器拒绝初始请求，并给客户端发送：正在使用摘要式身份验证和领域名称信息。
- (3) 运行 IIS 的服务器向客户端 IE 浏览器报告使用的是摘要式身份验证，而不是高级摘要式身份验证，这是因为对于摘要式身份验证和高级摘要式身份验证而言，运行 IIS 的服务器和客户端之间使用相同的摘要式身份验证算法。
- (4) IE 提示用户输入凭据（用户名和密码，对话框参见图 2-49 所示），然后，IE 浏览器合并这些凭据和领域名称以创建一个 MD5 哈希，并向运行 IIS 的服务器重新提交文件请求，此时还在 HTTP 请求的标题中发送 MD5 哈希。
- (5) 运行 IIS 的服务器收到客户端的哈希，并将其发送到域控制器，以进行验证。
- (6) 域控制器将客户端的哈希与 Active Directory 中存储的副本进行比较。如果哈希值匹配，则域控制器通知运行 IIS 的服务器该客户端已经过验证。然后，运行 IIS 的服务器将客

户端请求的文件发送到该客户端。

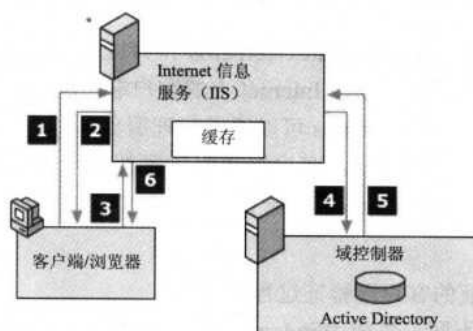


图 2-53 高级摘要式身份验证的客户端验证过程

3. 高级摘要式身份验证配置

摘要式身份验证方式的配置也是通过打开如图 2-46 和图 2-47 所示的对话框进行的。具体步骤如下。

(1) 在“用户访问需经过身份验证”栏中选择“Windows 域服务器的摘要式身份验证”复选项。

(2) 在“领域”文本框中键入领域的名称，或者单击【选择】按钮以浏览域。如果为所配置的站点、虚拟目录或文件夹启用了基本身份验证，则还可以使用“默认域”文本框。但是，对于高级摘要式身份验证而言，只有“领域”文本框是有效的。

(3) 同样依次单击【确定】按钮两次完成配置。

同样，可以在运行 IIS 的服务器上配置一个或多个领域名称。可配置领域的配置数据库级别也如上节的表 2-10 一样。

高级摘要式身份验证使用称为 UseDigestSSP 的配置数据库项。此配置数据库项是摘要式 and 高级摘要式安全支持提供程序接口 (SSPI) 代码之间的开关。如果已设置了该项，则有效的属性值只能是 1 (TRUE)、0 (FALSE) 或空。如果将该属性设置为 TRUE，则使用高级摘要式身份验证的新 SSPI 代码。在所有其他情况 (FALSE、空或者没有设置) 下，IIS 使用摘要式身份验证代码。

可以在配置数据库的 W3SVC 级别配置 UseDigestSSP 的配置数据库属性。子项从其上面的级别继承其配置。

2.5.10 集成 Windows 身份验证及配置

集成 Windows 身份验证（以前称为 NTLM 或 Windows NT 质询/响应验证）是一种安全的验证形式，因为在通过网络发送用户名和密码之前，先将它们进行哈希计算。当启用集成 Windows 身份验证时，用户的浏览器通过与 Web 服务器进行密码交换（包括哈希方式）来证明密码。

集成 Windows 身份验证是 Windows Server 2003 家族成员中使用的默认验证方法，它使用 Kerberos v5 验证和 NTLM 验证。如果在 Windows 2000 或更高版本域控制器上安装了 Active

78 网管员必读——网络应用（第2版）

Directory 服务，并且用户的浏览器支持 Kerberosv 5 验证协议，则使用 Kerberosv 5 验证，否则使用 NTLM 验证。

集成 Windows 身份验证包括 Negotiate、Kerberos 和 NTLM 验证方法。Negotiate（Kerberos 和 NTLM 的重新封装）非常适用于连接 Internet 上的客户端，因为 NTLM 可以通过防火墙，但通常会被代理服务器挡住；而 Kerberos 可以通过代理服务器，但通常会被防火墙挡住。

要成功地进行 Kerberosv 5 验证，客户端和服务端都必须可靠地连接到密钥分配中心（KDC），并且必须与 Active Directory 服务兼容。

1. 客户端验证过程

集成 Windows 身份验证的客户端验证过程如下。

（1）与基本身份验证不同，集成 Windows 身份验证开始时并不提示用户输入用户名和密码。客户机上的当前 Windows 用户信息可用于集成 Windows 身份验证。

（2）如果开始时的验证交换无法识别用户，则浏览器提示用户输入 Windows 账户用户名和密码，并使用集成 Windows 身份验证进行处理。

（3）IE 将继续提示用户，直到用户输入有效的用户名和密码或关闭提示对话框为止。

尽管集成 Windows 身份验证非常安全，但它仍然有如下两个限制。

- 只有 IE 2.0 和更高版本才支持这种验证方法。
- 它不能用于 HTTP 代理连接。

因此，集成 Windows 身份验证最适用于 Intranet 环境，在其中用户和 Web 服务器计算机位于相同的域中，并且管理员可以确保每个用户使用 IE 2.0 或更高版本。如果集成 Windows 身份验证由于用户凭据错误或其他问题而失败，则浏览器就会提示用户输入用户名和密码。

集成 Windows 身份验证可使用 Kerberos 密钥验证方式。在 Kerberos 身份验证服务对某个服务进行验证之前，该服务只能在一个账户对象上注册。如果服务实例的登录账户发生变化，则该服务必须使用新账户重新注册。因此，只有一个注册了该服务的应用程序池可以使用 Kerberos 进行验证。因此，在应用程序池的虚拟目录级别上，不能将站点彼此隔离。但是有一个解决办法：客户可以基于域名来隔离这些站点。例如，CompanynameHR.com 和 CompanynameSales.com。

2. 配置集成 Windows 身份验证

摘要式身份验证方式的配置也是通过打开如图 2-46 和图 2-47 所示的对话框进行的。具体步骤如下。

（1）在如图 2-47 所示的对话框中的“用户访问需经过身份验证”栏中选择“集成 Windows 身份验证”复选项。

（2）同样依次单击【确定】按钮两次完成配置。

2.5.11 证书身份验证

证书是用于服务器和从服务器请求信息的客户端的一种数字标识。它们的功能犹如护照，或其他官方的身份证（这些证件用于标识其持有人身份）。证书是 IIS 安全套接字层（SSL）功能的一部分，用于建立加密连接以通过该连接发送敏感信息。

证书包含通过网络确定身份（即称为身份验证的过程）所使用的信息。与验证的常见形

式一样，证书使 Web 服务器和用户在建立连接前能够互相进行身份验证。证书也包含加密值，或“密钥”，它们用于在客户端和服务器之间建立安全套接字层（SSL）连接。通过此连接发送的信息（例如信用卡号码）将被加密，这样未经授权的一方就不能截取和使用它。

在 SSL 中使用的证书有两种类型，每种类型的证书具有自己的格式和用途：服务器证书和客户端证书。“服务器证书”包含关于服务器的信息，该信息允许客户在共享敏感信息之前对服务器进行确认性识别。“客户端证书”包含关于请求访问站点的客户的个人信息，在允许客户访问站点之前，可以使用此证书对客户进行有效的标识。

要激活 Web 服务器的 SSL 安全功能，必须获得并安装有效的服务器证书。服务器证书即为数字标识，其中包含关于 Web 服务器及赞助服务器 Web 内容的机构的信息。用户可使用服务器证书来验证你的服务器，检查 Web 内容的有效性，以及建立安全连接。服务器证书还包含“公钥”，它用于创建客户端和服务器之间的安全连接。

作为一种标识方法，服务器证书成功与否取决于用户是否相信证书中所包含信息的有效性。例如，登录到公司网站的用户可能犹豫是否提供信用卡信息，尽管他（她）已经看到了公司服务器证书的内容。如果贵公司是一家新公司并且尚不知名，这种现象尤其明显。如果是这种情况，请考虑从证书颁发机构获取服务器证书。另外，根据其机构与网站用户的关系，可以发布自己的服务器证书。

1. 客户端证书

客户端证书是包含客户信息的电子文档。这些证书和服务器证书一样，不仅包含该信息，而且还包含构成 IIS 的 SSL 安全功能一部分的加密密钥。由于有了来自服务器和客户端证书的公钥或加密代码，对在开放网络（如 Internet）上传输数据进行加密和解密变得更为容易。

典型的客户端证书包含下面几项信息：用户的标识、证书颁发机构的标识、用于建立安全通信的“公钥”及确认信息（如截止日期和序列号等）。证书颁发机构提供不同类型的客户端证书，这些证书包含不同数量的信息（取决于要求的验证级别）。

可以对两种类型的验证使用 Web 服务器的安全套接字层（SSL）安全功能。可以使用“服务器证书”，允许用户在传送个人信息（如信用卡号码）之前进行网站验证。同样，也可以使用“客户端证书”对请求网站信息的用户进行验证。通过检查登录过程中用户 Web 浏览器提交的加密数字标识的内容进行 SSL 验证（用户从一个互相信任的第三方机构获取客户端证书）。服务器证书通常包含关于其公司及发证机构的信息。客户端证书通常包含关于用户和发证机构的识别信息。

2. 客户端证书映射

因为访问文件等资源时需要使用 Windows 用户账户，所以可以将客户端证书映射到 Web 服务器上的 Windows 用户账户。创建并启用证书映射后，每次用户使用客户端证书登录时，Web 服务器就会自动将用户与其相应的 Windows 用户账户关联起来。这样，就可以自动验证使用客户端证书登录的用户，而不必使用其他的验证方法，如基本身份验证、摘要式身份验证或集成 Windows 身份验证。可以将一份客户端证书映射到一个 Windows 用户账户，或者将多个客户端证书映射到一个账户。例如，如果在服务器上有几个不同的部门或企业并且它们都有自己的网站，则可以使用多对一映射将每个部门或公司的所有客户端证书映射到各自的网站。这样，每个站点仅对自己的客户提供访问。

80 网管员必读——网络应用（第2版）

因为证书配置比较复杂，且在一般的对外网站上比较少用，所以在此对其配置不做详细介绍。

2.5.12 .NET Passport 身份验证

.NET Passport 是一个用户身份验证服务，并且是 Microsoft .NET Framework 的一个组件。通过使用 .NET Passport 单次登录服务和快速购买服务，企业可以给客户提供一种快速、方便的方法来进行登录并在其站点上进行交易。可以使用 .NET Passport 单次登录服务将登录名映射到数据库中的信息，以便通过目标广告、促销信息和内容给 .NET Passport 成员提供具有个性化的 Web 体验。通过按这种方式使用 .NET Passport，可潜在地帮助留住客户，提高销售额及广告收入。

.NET Passport 使用标准 Web 技术来提供单次登录服务，如安全套接字层（SSL）、HTTP 重定向、Cookie、Microsoft JScript，以及强对称密钥加密。.NET Passport 与 IE 4.0 或更高版本，以及 Netscape Navigator 4.0 或更高版本兼容。此外，.NET Passport 与某些 UNIX 版本兼容。

.NET Passport 是一种用户身份验证服务，站点用户可使用该服务创建单次登录名和密码，从而方便地访问所有启用 .NET Passport 的网站和服务。启用 .NET Passport 的站点依靠 .NET Passport 中央服务器来验证用户，而不是主持和维护它们自己的专用身份验证系统。但是，.NET Passport 中央服务器并不授权或拒绝特定用户访问单个启用 .NET Passport 的站点。而是由网站来控制用户的权限。

.NET Passport 也可以将用户信息存储在 .NET Passport 服务器上的加密配置文件（也称为“注册”）中。当 .NET Passport 用户注册参与站点时，就会与该站点共享其个人信息以加快注册过程。当 .NET Passport 用户再次登录到该站点时，其 .NET Passport 配置文件可允许访问该站点上的个人账户或服务。

1. .NET Passport 扩展

.NET Passport 单次登录服务与当前 Web 上基于表单的常用身份验证模型类似。.NET Passport 网络扩展了这种模型以用于一组分布式的参与站点，同时有助于保留成员的保密性和安全性，以及适当自定义和署名登录的功能。特别地，.NET Passport 使用以下方法来扩展基于表单的身份验证模型。

- 登录、注销和注册页是集中主持的，而不是每个单独站点特有的。
- 可以广泛地对 .NET Passport 进行共同署名以符合站点外观。当在客户端浏览器中显示集中主持的页时，可以从站点直接为共同署名材料提供服务，并且共同署名材料包含在这些页中。
- 对于需要额外安全性能以交换凭据或其他信息的集中主持的页，始终使用安全套接字层（SSL）为这些页提供服务。
- 所有 .NET Passport 登录和核心配置文件 Cookie 均经过严格加密。每个参与网站收到唯一的加密密钥以有助于确保信息的保密性。
- 中央 .NET Passport 服务器将加密的登录和配置文件信息返回给你的站点，可随后使用这些信息写入本地 Cookie，从而避免在后续界面查看时重定向回中央 .NET Passport 服务器。

- 在站点之间移动时，成员不需要重新键入其登录名称和密码。启用.NET Passport 的站点在.NET Passport 中央服务器的域中发布一组加密的 Cookie，以简化站点间静态和无缝登录的过程。但是，站点可能仍然选择始终强制将成员重定向到.NET Passport 登录，并且在第一次查看其站点时进行身份验证。
- 参与站点从未收到成员的密码。实际上，身份验证 Cookie 是一对加密的时间戳（用于声明成员登录的时间）。当成员通过单击.NET Passport 注销链接选择注销时，就会将它们重定向到一个中心页，该页启用了从成员会话期间访问的所有站点中删除所有.NET Passport Cookie 的操作。
- 参与网站和中央.NET Passport 服务器之间没有服务器到服务器的实时通信，所有信息交换是通过客户端的浏览器进行的（使用 HTTP 重定向、查询字符串上的加密信息及 Cookie）。仅当.NET Passport 的服务器端对象（在.NET Passport SDK 中提供）定期下载和本地缓存集中主持的 XML 配置文件时，才进行服务器到服务器通信；此 XML 文件包含所有.NET Passport 服务器的当前 URL 和当前配置文件架构。

2. 在 IIS 中设置.NET Passport

在为网站设置.NET Passport 身份验证之前，需要对 IIS 进行针对.NET Passport 预生产服务器的测试。在完成这些过程后，则可确信 IIS 服务器和.NET Passport 服务器之间能够正确通信，经站点则注册了.NET Passport（可能会涉及到签署表单和协议）并且网站具有正确的站点标识。对于要启用.NET Passport 身份验证的每个网站，必须完成每个过程。

在 Windows Server 2003 家族成员上启用.NET Passport 身份验证后，默认.NET Passport SecureLevel（安全级别）设置为 10。这意味着使用.NET Passport 身份验证（和默认设置）的新站点需要安全套接字层（SSL）服务器证书。可通过更改注册表值来更改站点的 SecureLevel 设置。

更改默认网站的 SecureLevel 设置的方法是在注册表中给以下项输入新的值：HKEY_LOCAL_MACHINE\Software\Microsoft\Passport\SecureLevel。

更改非默认网站以外任何网站的 SecureLevel 设置的方法是在注册表中给以下项输入新的值：HKEY_LOCAL_MACHINE\Software\Microsoft\Passport\Sites\<Site Name>\SecureLevel。

3. 启用.NET Passport 身份验证

在启用.NET Passport 后，发往 IIS 的请求在查询字符串或 Cookie 中必须包含.NET Passport 凭据。凭据还必须是有效的，即票据没有过期。如果 IIS 没有检测到.NET Passport 凭据，则将请求重定向到.NET Passport 登录页。

.NET Passport 使用 Cookie，它包含的信息可能会泄密。不过，可以通过安全套接字层（SSL）连接使用.NET Passport 验证，这可减少遭受重播攻击的可能性。

在网站上启用.NET Passport 验证的步骤如下。

（1）在相应的网站上打开如图 2-47 所示的对话框。选中“.NET Passport 身份验证”复选选项。.NET Passport 验证用户凭据的方式与其他验证方法完全不同，因此，不能将.NET Passport 与其他验证方法结合使用。在选择.NET Passport 身份验证后，不能使用所有其他的验证方法。

（2）单击【确定】按钮完成配置。

2.5.13 UNC 身份验证

通用命名约定（UNC）验证方法也称为“UNC Passthrough 验证”，它确定获得远程计算机上 UNC 共享访问使用的凭据。从 IIS 6.0 开始，UNC 验证使用以下方法查看请求用户和配置数据库 UNCUserName 和 UNCPassWord 属性中存储的凭据，以确定传送到具有 UNC 共享的计算机上的凭据。

如果指定了 UNCUserName（非空），并且 UNCPassWord 有效，则将配置数据库用户凭据作为访问的用户标识发送到远程共享；如果指定了 UNCUserName（非空），但是 UNCPassWord 无效，则向客户端发送“500 内部服务器错误：用户名或密码无效”消息；如果 UNCUserName 为空，则将请求用户的凭据（用于已验证请求的一组验证的凭据或用于匿名请求的 IUSR_computername 凭据）作为访问的用户标识发送到远程共享。

在 IIS 6.0 中，不再将 UNCAuthenticationPassthrough 配置数据库项用于 UNC 验证。

2.5.14 访问控制

适当地控制对 Web 和 FTP 内容的访问是安全运行 Web 服务器的关键。使用 Windows 和 IIS 中的安全功能，可以有效地控制用户访问 Web 和 FTP 内容的方式。可以控制多级访问，从整个网站和 FTP 站点到单独的文件。

每个账户均被授予用户特权和权限。用户特权是指在计算机或网络上执行特定操作的权力。而权限是与对象（如文件或文件夹）关联的规则，用于控制那些账户可以获得对象的访问权限。用户权力和特权是在组策略中配置的，具体的配置方法参见本系列丛书的《网管员必读——网络管理》一书。

可以通过正确地配置 Windows 文件系统和 Web 服务器安全功能来控制用户对 Web 服务器的访问。当用户试图访问 Web 服务器时，服务器执行几个访问控制进程来识别用户并确定允许的访问级别。具体的访问控制原理如图 2-54 所示。

下面是以上访问控制过程的简述。

- （1）客户请求服务器上的资源。
- （2）将依据 IIS 中 IP 地址限制检查客户机的 IP 地址。如果 IP 地址是禁止访问的，则请求就会失败并且给用户返回“403 禁止访问”消息。
- （3）如果服务器要求身份验证，则服务器从客户端请求身份验证信息。浏览器既提示用户输入用户名和密码，也可以自动提供这些信息。
- （4）IIS 检查用户是否拥有有效的 Windows 用户账户。如果用户没有提供，则请求就会失败并且给用户返回“401 拒绝访问”消息。
- （5）IIS 检查用户是否具有请求资源的 Web 权限。如果用户没有提供，则请求就会失败并且给用户返回“403 禁止访问”消息。
- （6）添加任何安全模块，如 ASP.NET 模拟。
- （7）IIS 检查有关静态文件、Active Server Pages（ASP）和通用网关接口（CGI）文件上资源的 NTFS 权限。如果用户不具备资源的 NTFS 权限，则请求就会失败并且给用户返回“401 拒绝访问”消息。

(8) 如果用户具有 NTFS 权限，则可完成该请求。

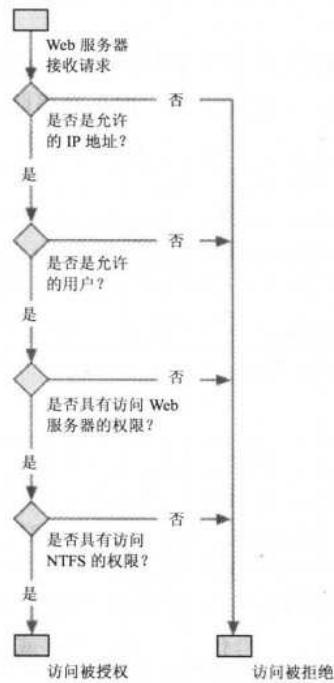


图 2-54 访问控制原理

2.5.15 NTFS 权限

强烈建议应用程序服务器使用 NTFS 文件系统。与 FAT 和 FAT32 相比，NTFS 是更强大和更安全的文件系统。可以使用 NTFS 限制对 Web 服务器文件和目录的访问，也可以配置给某个用户或组授予的服务器文件和目录访问级别。除了允许使用比 FAT 更大的卷大小外，NTFS 还具有如表 2-11 所示的其他优点。

表 2-11 NTFS 与 FAT 格式的比较

NTFS	FAT
允许管理员使用 NTFS 权限保护目录和文件。可以在文件或目录级别设置权限	不允许管理员保护目录和文件
支持文件加密（它可大大增强文件的安全性）	不支持文件加密
允许管理员启用 Web 分布式创作和版本控制（WebDAV）属性	不允许管理员启用 WebDAV 属性
支持基于 Active Directory 和域的安全功能	不支持基于 Active Directory 和域的安全功能

配置时只需在相应网站，或网站文件夹上单击鼠标右键，在弹出的快捷菜单中选择【权限】命令，在打开的“权限”对话框中即可配置。当然也可以在资源管理中通过相应文件夹的右键属性对话框中选择“安全”选项卡配置。具体的 NTFS 访问权限的配置方法参见本系列丛书的《网管员必读——网络管理》一书。

2.5.16 TCP/IP 端口筛选

筛选 TCP/IP 端口允许控制到达服务器和网络设备的通信类型。虽然在 Internet 访问点部署的防火墙通常用于限制流入专用网络的流量，但是网络防火墙可能无法保护服务器不被“后门”攻击或内部攻击，这些攻击源于专用网络内的恶意用户。

TCP/IP 端口筛选是启用或禁用计算机或网络设备上的传输控制协议（TCP）端口和用户数据报协议（UDP）端口的选择性操作。与其他安全性操作结合使用，将端口筛选器应用于 Intranet 和 Internet 服务器使得那些服务器隔离基于 TCP/IP 的安全性攻击，包括恶意用户的内部攻击。

要预防这种攻击，可以在单独的服务器上配置端口筛选器。这样提供了额外的保护层来预防众多的基于 TCP/IP 的安全性攻击。

1. TCP 和 UDP 端口

Internet 或 Intranet 主机（例如，基于 TCP/IP 网络上的计算机或网络设备）使用 Internet 协议（IP）地址和端口号的组合来与运行在其他 Internet 或 Intranet 主机上的应用程序或服务进行通信。IP 地址和端口号合起来组成套接字。由于 TCP/IP 主机被指派给唯一的 IP 地址，并且标准的基于 TCP/IP 的应用程序和服务通常使用特定的 TCP 或 UDP 端口号，因此套接字可以定向运行在特定主机上的特定应用程序或服务之间的通信。


在 TCP 或 UDP 包头中标识的端口号代表了使用 TCP 或 UDP 的特定应用程序和服务的传输协议地址。例如，在默认情况下，HTTP 服务使用 TCP 端口 80，Telnet 使用 TCP 端口 23，简单网络管理协议（SNMP）使用 UDP 端口 161。

Internet 指定的编号机构（IANA）将 TCP 和 UDP 端口分成 3 类，如表 2-12 所示。

表 2-12 TCP 和 UDP 端口分类

端口类别	端口号范围	描述
已知端口	0~1023	通常由标准系统进程或程序使用，由带有管理凭据的用户执行，由 IANA 指派
注册端口	1024~49151	由普通用户进程或程序使用，由普通用户执行，IANA 不指派这些端口，但是注册表将它们作为一个便利用于 TCP/IP 社区
动态或专用端口	49152~65535	用于专用应用程序、客户端进程，或动态分配端口号的其他进程的未分配的或未注册的端口

通常，TCP 或 UDP 进程的服务器端监听相关的已知端口号。进程的客户端使用已知端口号，或者使用仅为进程中指派的动态分配的端口号（更常见）。



注意

Windows 套接字应用程序可以使用 GetServByName ()函数来通过名称引用端口号。名称通过 systemroot\System32\Drivers\Etc 文件夹的 services 文本文件中指派的值被解析到端口号。

要启动服务器使用的应用程序和服务之间的通信，必须确保已启用了相关的端口。但是，内部网络上的恶意用户可以试图利用已启用的端口来攻击服务器，因此你应该禁用服务器上不用的 TCP 和 UDP 端口。这样可以减少攻击服务器的通道，并且提高连接到服务器的主机的安全性。



注意

基于服务器的端口筛选不是用来防止服务器和网络免受基于 TCP/IP 的安全性攻击的唯一方法。为了提供更完整的网络安全解决方案，还应该在互联网访问点部署网络防火墙软件。网络防火墙允许用户建立特定的规则来控制与服务器和其他网络资源通信的主机、网络、应用程序以及服务的类型。与其他安全性工具和操作组合使用，基于服务器的端口筛选和网络防火墙提供了抵御网络安全攻击的第一线防御。

2. Internet 服务的端口分配

使用传输控制协议（TCP）的应用程序进程可以使用 65535 个端口号。使用用户数据报协议（UDP）的应用程序进程可以使用相同数目的端口。

表 2-13 列出了一些通常用于 Internet 服务的进程的默认 TCP 端口号。

表 2-13 常用于 Internet 服务的进程的默认 TCP 端口号

默认 TCP 端口号	Internet 服务
20	文件传输协议（FTP）数据通道
21	文件传输协议（FTP）控制通道
23	Telnet（在某些 Intranet 或 Internet 服务器上启用）
25	简单邮件传输协议（SMTP）
80	用于万维网的超文本传输协议（HTTP）
119	网络新闻传输协议（NNTP）
443	用于安全万维网的 TLS/SSL 上的超文本传输协议（HTTPS）
563	TLS/SSL 上的网络新闻传输协议（NNTPS）



注意

通过使用多种静态或动态的 UDP 和 TCP 端口，或通过使用单个端口（具体情况依配置而定），Windows Media 服务（WMS）可以以单播或多播 IP 的方式提供流媒体服务。还可以通过使用默认的 HTTP 端口（TCP 端口 80）将 WMS 配置为提供流媒体服务。

常用于 Internet 服务的进程的已知 UDP 端口号有如下两个。

- 53：域名系统（DNS）名称查询（支持某些 Internet 服务）
- 161：简单网络管理协议（SNMP）



说明

服务器可能需要支持附加的进程，包括支持针对于所处环境的远程管理工具或应用程序进程。在配置端口筛选器前，请仔细清点每个服务器上使用的进程。有关 Windows Server 2003 家族使用的 TCP 和 UDP 端口号列表，请参阅 systemroot\System32\Drivers\Etc 文件夹中的 services.txt 文件。

3. 端口筛选工具

Windows Server 2003 家族包含在单个服务器上筛选端口和数据包的多个工具。还可以使用 Internet Security and Acceleration Server（可独立使用）在互联网出口点筛选网络流量。

表 2-14 列出了可以用于在服务器或网络上筛选流量的工具。

表 2-14 在服务器或网络上可用的筛选流量工具

筛选工具	描述
Internet 协议安全 (IPSec) 筛选策略	支持基于策略的监控状态的分组筛选器规则，此规则可用于 IPSec 身份验证和加密以便提供可靠的端对端安全性。如果你的组织已经部署了 IPSec，建议使用此工具
Internet 连接防火墙 (ICF)	启用基于可配置服务定义的监控状态的筛选器。支持日志记录和通知服务。如果你的组织尚未部署 IPSec，建议使用此工具。在 Windows XP 和 Windows Server 2003 R2 系统中，“Internet 连接防火墙 (ICF)”已改为“Windows 防火墙”
Internet 验证服务 (IAS)	提供包括流量筛选在内的网络访问控制服务，用于无线网络、远程访问、虚拟专用网络、Internet 资源和 extranet
TCP/IP 筛选	限制无状态分组和协议筛选。不建议使用此工具。IPSec 和 ICF 提供了更加有用和可靠的监控状态的筛选器
Internet Security and Acceleration Server	作为可用的独立产品（不包含在 Windows Server 2003 家族中）。包括高级网络防火墙软件，使用此软件能够为计算机和网络设备配置复杂的流量和应用程序筛选规则

要有效地使用 TCP 和 UDP 端口，请配置筛选工具以便接受通过服务器应用程序要求的每个端口的请求，并且拒绝来自所有其他 TCP 或 UDP 端口的请求。仔细确定应用程序的 TCP、UDP 端口要求，并且设置相应的筛选工具，这样将避免出现对你当前尝试提供的服务的拒绝访问错误。筛选掉所有其他的 TCP 和 UDP 端口将消除不必要的易受攻击的隐患。

4. 端口筛选配置

在此仅介绍两种最基本、最容易实现的端口筛选方法，那就是利用“Windows 防火墙”和“TCP/IP 筛选”两种方式的具体配置方法。

在“Windows 防火墙”中配置筛选端口的方法如下。

- (1) 在相应的网络连接上，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“高级”选项卡，如图 2-55 所示。
- (2) 单击【设置】按钮，在打开的对话框中选择“例外”选项卡，如图 2-56 所示。
- (3) 单击【添加端口】按钮，打开如图 2-57 所示的对话框进行。添加端口后，在如图 2-56 所示的列表框中选择新添加的端口选项，这样 Windows 防火墙就会阻止其他未添加到如图 2-56 所示的对话框的“程序和服务”列表中，并且没有选取端口的选项，达到筛选的目的。

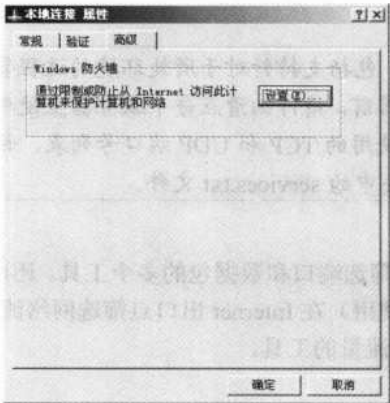


图 2-55 网络连接属性对话框“高级”选项卡



图 2-56 “Windows 防火墙”对话框“例外”选项卡

利用“TCP/IP 筛选”功能实现端口筛选的配置方法如下。

(1) 在相应的网络连接上，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，然后在打开的对话框中选择“常规”选项卡，如图 2-58 所示。

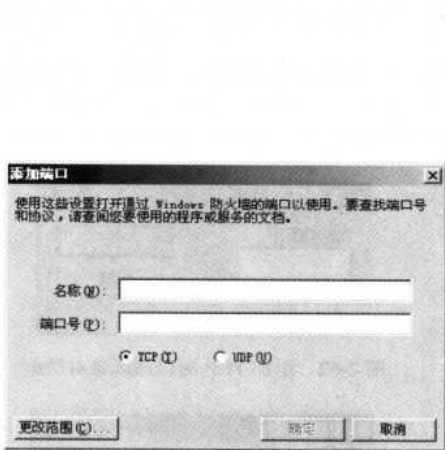


图 2-57 “添加端口”对话框

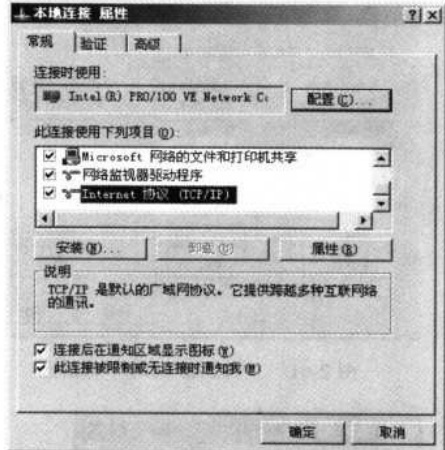


图 2-58 网络连接属性对话框“常规”选项卡

(2) 选择“Internet 协议 (TCP/IP)”选项，单击【属性】按钮，打开如图 2-59 所示的对话框。

(3) 单击【高级】按钮，在打开的对话框中选择“选项”选项卡，如图 2-60 所示。

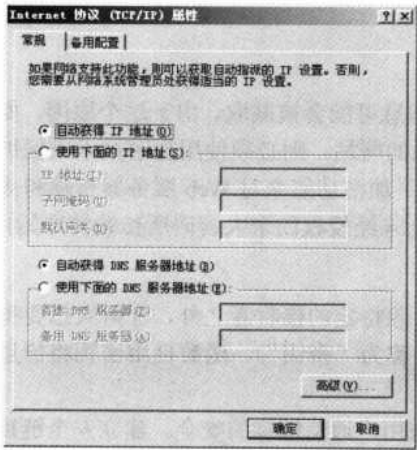


图 2-59 “Internet 协议 (TCP/IP) 属性”对话框

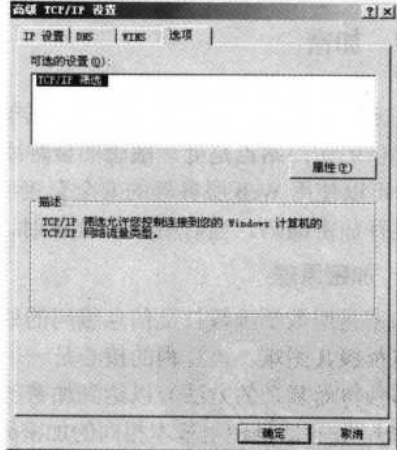


图 2-60 “高级 TCP/IP 设置”对话框

(4) 选择列表框中的“TCP/IP 筛选”选项，然后单击【属性】按钮，打开如图 2-61 所示的对话框。在这里首先要选择“启用 TCP/IP 筛选（所有适配器）”复选项，然后在下面对应的端口或协议栏中选择“只允许”单选项。单击【添加】按钮，如果选择的是“TCP 端口”栏，则打开的是如图 2-62 所示的对话框，在其中的文本框中输入允许通信的 TCP 端口号；如果选择的是“UDP 端口”栏，则打开的是如图 2-63 所示的对话框，在其中的文本框

中输入允许通信的 UDP 端口号；如果选择“IP 协议”栏，则打开的是如图 2-64 所示的对话框，在其中的文本框中输入允许通信的 IP 协议号。当然，配置端口筛选只需在“TCP 端口”，或者在“UDP 端口”栏中配置即可。

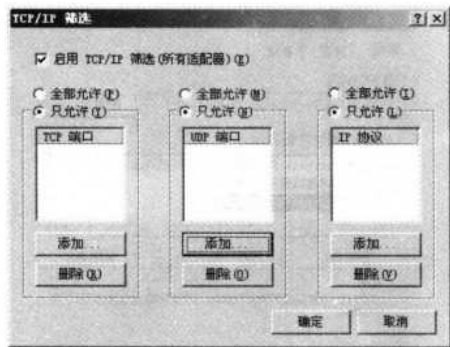


图 2-61 “TCP/IP 筛选”对话框



图 2-62 添加 TCP 端口筛选器对话框

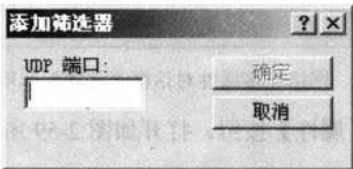


图 2-63 添加 UDP 端口筛选器对话框

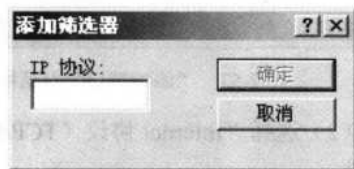


图 2-64 添加 IP 协议号筛选器对话框

2.5.17 加密

在未保护的网路（如 Internet）上传输的敏感信息可能会被截取。由于这个原因，如果为用户提供的是处理敏感的金融或个人信息的网站，则必须使用加密技术来保护这些数据。可以使用 Web 服务器的安全套接字层（SSL）加密功能来对 Web 服务器传输和接收的信息进行加密编码。当启用 SSL 加密时，可以防止未经授权的个人解码所传输的原始内容。

1. 加密原理

加密是用数学函数打乱信息编码的处理过程，除特定的接收者之外，任何人想要得到原始信息都极其困难。该过程的核心是一个数学值（称为“密钥”），函数使用密钥将信息打乱（采用独特而复杂的方法）以达到加密的目的。

Web 服务器也使用基本相同的加密处理保护与用户通信链接的安全。建立安全链接后，Web 服务器和用户的 Web 浏览器使用专门的“会话”密钥来加密和解密信息。例如，当验证过的用户尝试从要求安全通道的网站下载文件时，Web 服务器使用会话密钥加密该文件及关联的 HTTP 头。Web 浏览器在接收到加密的文件以后，使用同一会话密钥的副本来恢复该文件。

这种加密方法虽然安全，但具有一个内在的缺点：在创建安全链接的过程中，会话密钥副本可能会通过不安全的网路进行传送。这意味着如果计算机破坏者想要破坏该链接，只需截取并窃得该会话的密钥。因此为保证不出现这种情况，Web 服务器还需执行附加的加密方法。

2. 公钥加密原理

Web 服务器安全套接字层（SSL）安全功能使用一种称为“公钥”的加密技术来保护会话密钥，以免在传输过程中被截取。公钥加密使用两个附加密钥（即“私钥”和“公钥”），其工作原理如下。

- （1）用户的 Web 浏览器与 Web 服务器建立安全（https://）通信链接。
 - （2）用户的 Web 浏览器和服务端进行协商，确定用于保证通信安全的加密程度。
 - （3）Web 服务器将其公钥发送给浏览器。
 - （4）Web 浏览器使用服务器公钥对生成会话密钥过程中所使用的信息进行加密，并将其发送到服务器。
 - （5）服务器则使用私钥解密该消息，然后生成会话密钥，将其用公钥加密，再发送给浏览器。
 - （6）Web 服务器和浏览器此后便使用会话密钥加密和解密传输的数据。
- 整个加密过程中密码的变化如图 2-65 所示。

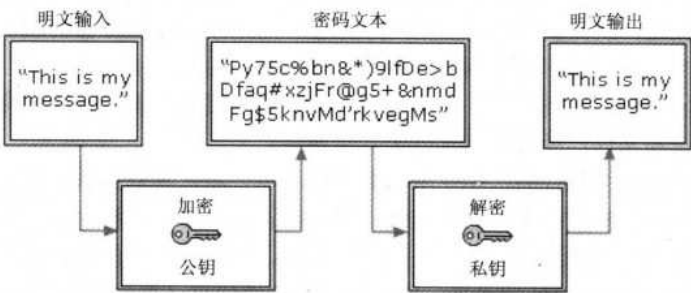


图 2-65 公钥加密中的密码变化过程

注意 私钥在保证通信链接安全方面担当起了一个重要的角色。应紧密防范以保护私钥避免丢失或被窃取。如果怀疑私钥可能已被解密，请通知证书颁发机构，使用 Web 服务器证书向导创建新的证书请求，然后获取新的服务器证书。

3. 会话密钥加密强度

会话密钥的“强度”与组成会话密钥文件的二进制“位”的位数成正比。这意味着位数较多的会话密钥具有更强的安全性，要强制解密也更加困难。

当用户尝试与你的服务器建立安全通信通道时，用户浏览器必须协商好加密技术可能采用的最强级别，或称会话密钥强度，这可以保护通过该通道进行的通信安全。这意味着 Web 服务器和用户浏览器必须对会话密钥具有一致的加密和解密功能。例如，当 Web 服务器配置成需要最小 40 位（默认）加密长度的会话密钥时，希望保证连接安全的用户也必须具有能处理 40 位会话密钥信息的 Web 浏览器。

4. 服务器网关加密

服务器网关加密（SGC）使用 128 位加密为金融机构提供了全球金融交易解决方案。SGC 是安全套接字层（SSL）的扩展，它允许拥有 IIS 出口版本的金融机构可使用强加密。

SGC 不要求在客户端浏览器上运行应用程序，并且可由 IIS 4.0 或更高版本的标准出口版

90 网管员必读——网络应用（第2版）

本使用，配置了 SGC 的服务器可以方便地进行 128 位和 40 位加密。虽然 SGC 功能已内建到 IIS 4.0 及以后版本中，但是使用 SGC 时还需要特殊的 SGC 证书。联系证书颁发机构以获取可用信息。

5. 可选的加密服务提供程序

通过使用可选的加密提供程序（CSP），可以选择 Microsoft 或第三方加密提供程序来处理加密和证书管理。每个加密提供程序可以创建公钥和私钥以加密和解密数据。私钥存储在服务器上的文件系统、PCI 卡、智能卡或者注册表中，这是因为它用于 Microsoft 安装的两个默认提供程序：Microsoft DHS Channel 加密提供程序和 Microsoft RSAS Channel 加密提供程序。每个提供程序的 Microsoft 加密 API（CryptoAPI）包含相同的方法和属性。因此，可以在提供程序之间切换，而无须重新编写代码。

6. 启用加密

在访问限制的网站、目录或文件之前，可以要求用户建立与服务器之间的加密通道（“https://”，而非“http://”）。但是，使用加密通道要求用户 Web 浏览器和 Web 服务器都支持所使用的加密策略，以保证通道的安全。特别地，当启用 Web 服务器的默认安全通信设置时，要求用户的 Web 浏览器支持长度为 40 位或 40 位以上的会话密钥。

当设置特定网站的安全属性时，自动为属于该站点的目录和文件设置同样的安全属性，除非某些单独目录和文件已经提前设置好了安全属性。

尝试设置网站的安全属性时，Web 服务器将提示用户是否具有重新设置单独的目录和文件属性的权限。如果选择重新设置这些属性，先前设置的安全属性将由新的设置所替代。该情况同样适用于为包含子目录或文件（在以前已设置了安全属性）的目录设置安全属性。

为了保证 Web 服务器的性能水平，应考虑只对敏感信息（如财务交易等）使用 SSL 加密。加密传输会明显降低传输速率和服务器性能。

在启用加密之前，必须安装一个有效的服务器证书。如果要求在 IIS 6.0 中加密，请先在服务器上配置中启用安全套接字层（SSL）的步骤。

7. 在服务器上配置 SSL

可以在 Web 服务器上配置安全套接字层（SSL）安全功能以检验内容完整性、用户标识和加密网络传输。Web 服务器要求有效的服务器证书以建立 SSL 通信。使用 Web 服务器证书向导生成可发送到证书颁发机构的证书请求文件（默认情况下为 NewKeyRq.txt），或生成对在线证书颁发机构（如 Microsoft 证书服务）的请求。

如果未使用 Microsoft 证书服务颁发自身的服务器证书，则必须由第三方证书颁发机构批准你的请求并给予颁发服务器证书。根据服务器证书提供的标识保证级别，可能需要等待几天到几个月，然后证书颁发机构才会批准你的请求并发送证书文件。每个网站只能有一个服务器证书。在收到服务器证书文件后，请使用向导安装该文件。安装进程将证书附加或“绑定”到网站。

在 Web 服务器上设置 SSL 的步骤如下。

（1）在 IIS 管理器中，展开本地计算机，然后展开“网站”文件夹。在要使用 SSL 保护的网站或文件上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，然后在打开的对话框中选择“网站”选项卡，如图 2-66 所示。

(2) 在“网站标识”栏中单击【高级】按钮，打开如图 2-67 所示的对话框。在“此网站的多个标识”下面，确保将网站的 IP 地址分配给端口 443（这是安全通信的默认端口），如果没有，则选择相应标识项，然后单击【编辑】按钮修改。最后两次单击【确定】按钮退出。要为此网站配置其他的 SSL 端口（可选），请在“此网站的多个标识”下面单击【添加】按钮，在打开的对话框中添加即可。



图 2-66 网站属性对话框“网站”选项卡

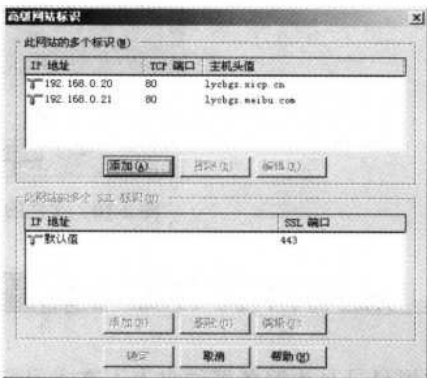


图 2-67 “高级网站标识”对话框

(3) 选择“目录安全性”选项卡（配置网站属性时，参见图 2-46），或“文件安全性”选项卡（配置文件属性时，如图 2-68 所示）的“安全通信”栏中单击【编辑】按钮，打开的对话框分别如图 2-69 和图 2-70 所示。

对比图 2-69 和图 2-70 两个对话框可见，两者非常相似，只是网站的安全通信可以启用证书信任列表，而文件的安全通信无须配置证书信任列表，因为它是继承网站这一属性的。

(4) 选中“要求安全通道（SSL）”复选项。如果要启用 SSL 客户端证书验证和映射功能，请选择“启用客户端证书映射”复选项，然后单击【编辑】按钮。在打开的对话框中进行配置。具体配置过程同样涉及到服务器证书，过程比较复杂，且比较少用，所以在此不作详细介绍。有需要的读者可以参见本系列图书的《网管员必读——网络安全》一书。

如果要求 128 位的密钥加密，则用户必须使用支持 128 位加密的 Web 浏览器。

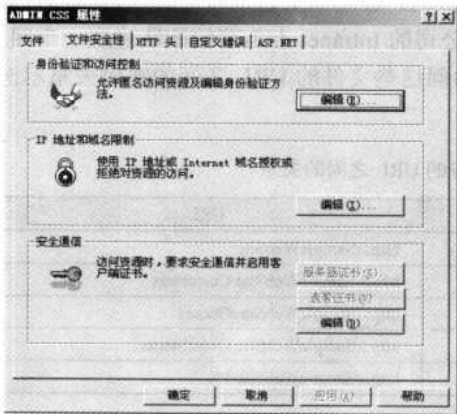


图 2-68 文件属性对话框“文件安全性”选项卡

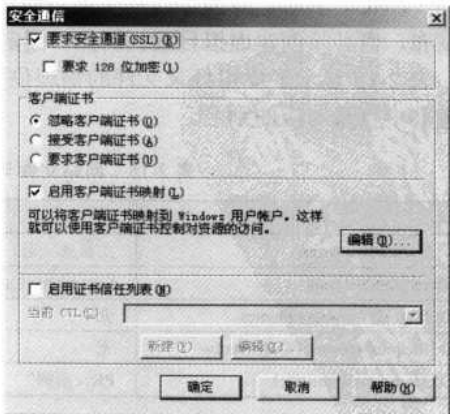


图 2-69 网站的“安全通信”对话框

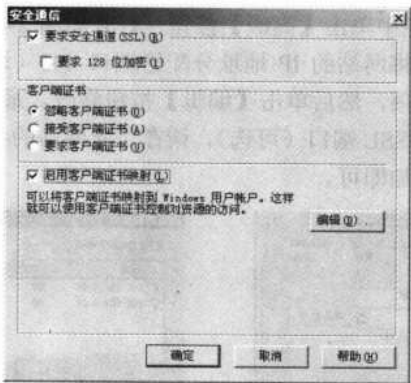


图 2-70 文件的“安全通信”对话框

2.6 虚拟目录创建与配置

虚拟目录是为服务器硬盘上不在主目录下的一个物理目录或者其他计算机上的主目录而指定的好记的名称，或“别名”。虚拟目录不在网站服务器主目录下，但又为网站服务器提供了资源，是整个网站文件的一部分。但在这里要注意的是，这个目录可以与网站主目录在同一主机上，只是不同目录而已，当然更多的情况是与网站主目录不在同一主机上，在网络中的其他计算机上。

因为别名通常比物理目录的路径短，更便于用户输入，所以在网站配置时不是直接指向相应虚拟目录的完全路径，而是用一个别名来替代。同时，使用别名还更加安全，因为用户不知道文件在服务器上的物理位置，所以无法使用该信息来修改文件。通过使用别名，还可以更轻松地移动站点中的目录。无须更改目录的 URL，而只需更改别名与目录物理位置之间的映射。

如果网站包含的文件位于非主目录中，或在其他计算机上，就必须创建虚拟目录，以将这些文件包含到你的网站中。要使用另一台计算机上的目录，必须指定该目录的通用命名约定的（UNC）名称，并为访问权限提供用户名和密码。若要从主目录以外的任何其他目录进行发布，也必须创建虚拟目录。例如，假定要在公司的 Intranet 上为营销团队建立一个网站。

表 2-15 显示了虚拟目录文件的物理位置与访问这些文件的 URL 之间的映射关系示例，注意其中目录对应的别名。

表 2-15 网站文件与其对应的 URL 之间的关系

物理位置	别名	URL
C:\inetpub\wwwroot	主目录（无）	http://SampleWebSite
\\Server2\SalesData	Customers（示例）	http://SampleWebSite/Customers
D:\inetpub\wwwroot\Quotes	无	http://SampleWebSite/Quotes
D:\inetpub\wwwroot\OrderStatus	无	http://SampleWebSite/OrderStatus
D:\Marketing\PublicRel	PR（示例）	http://SampleWebSite/PR

2.6.1 虚拟目录的创建

要从主目录以外的其他目录中进行发布，就必须创建虚拟目录。虚拟目录不包含在主目录中，但在显示给客户浏览器时就像位于主目录中一样。

对于简单的网站，可能不需要添加虚拟目录。只需将所有文件放在该站点的主目录中即可。如果站点比较复杂，或者需要为站点的不同部分指定不同的 URL，则可以根据需要添加虚拟目录。若要从多个站点访问某个虚拟目录，必须为每个站点添加虚拟目录。

创建或删除虚拟目录有以下 3 种方法。

- 使用 IIS 管理器（无论是使用虚拟目录创建向导，还是通过导入配置文件都可以）。
- 使用 Windows 资源管理器（这个方法需要你的硬盘格式化成 NTFS 文件系统）。
- 使用 iisvdir.vbs 管理脚本。

下面分别予以介绍。

1. 在 IIS 管理器中创建虚拟目录

（1）在 IIS 管理器中添加虚拟目录的网站（也可以是子网站）上单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【虚拟目录】命令，打开如图 2-71 所示向导对话框首页。

（2）单击【下一步】按钮，打开如图 2-72 所示的对话框。在“别名”文本框中键入虚拟目录的名称。这时用户键入的名称，应当有代表性，且简短、易于键入。

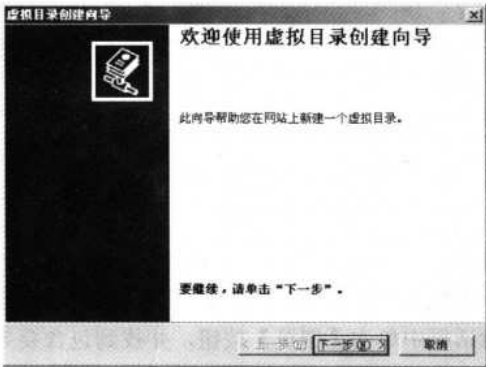


图 2-71 “欢迎使用虚拟目录创建向导”对话框

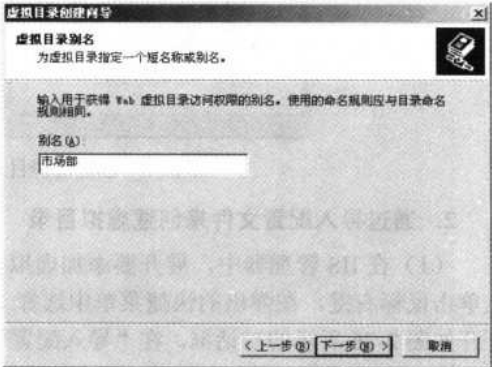


图 2-72 “虚拟目录别名”对话框

（3）单击【下一步】按钮，打开如图 2-73 所示的对话框。在“目录”文本框中键入，或单击【浏览】按钮在打开的窗口中找到虚拟目录所在的物理目录，这才是虚拟目录的真正位置所在。注意，此处只能选择目录，不能选择具体文件。最好是在 NTFS 文件格式的磁盘下，这样更加安全，因为可以配置文件夹的用户访问权限。

（4）单击【下一步】按钮，打开如图 2-74 所示的对话框。在这里设置网站用户访问该虚拟目录的权限，普通用户一般只需具有“读取”权限。具体权限说明在本章前面介绍网站创建时已有介绍，在此不再赘述。

（5）单击【下一步】按钮，打开一个向导完成对话框。单击其中的【完成】按钮完成虚拟目录的创建向导。此时会在 IIS 管理器控制台相应网站上显示新建的虚拟目录，如图 2-75

所示。

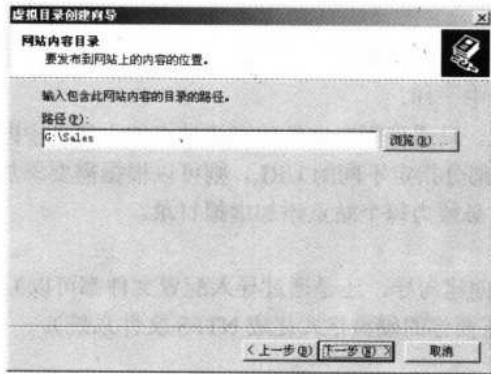


图 2-73 “网站内容目录”对话框

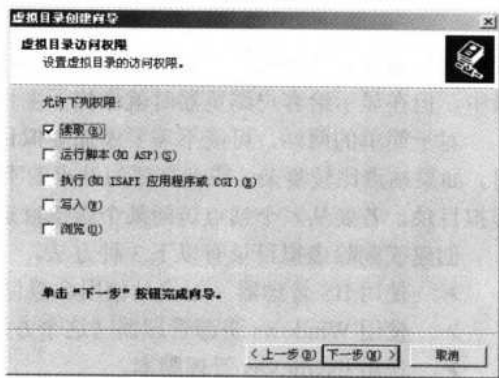


图 2-74 “虚拟目录访问权限”对话框



图 2-75 创建虚拟目录后的 IIS 管理器控制台

2. 通过导入配置文件来创建虚拟目录

(1) 在 IIS 管理器中，展开要添加虚拟目录的网站，在其中要创建虚拟目录的“网站”上单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【虚拟目录】（来自文件）命令，打开如图 2-76 所示的对话框。在“导入配置”对话框中单击【浏览】按钮，并找到包含要导入的虚拟目录配置的文件（.XML 格式）。



在导入配置文件前，必须从现有的 Web 应用程序池或网站导出配置文件。在 IIS 管理器中导出配置文件是采用【文件】菜单下的【将配置保存到一个文件】菜单项。导出的配置将存储为配置数据库 XML 配置文件，配置文件导出后，你可以将其导入到同一 Web 服务器的其他位置，或导入到其他的 Web 服务器。

(2) 选择好虚拟目录文件后，单击【读文件】按钮定位配置文件，系统会自动将包含在当前所选 XML 配置文件中的所有配置导入到此列表框。在打开的列表框中选择要导入的虚拟目录配置，然后单击【确定】按钮即可导入配置。这样，也会在当前选定的级别下面创建虚拟目录。

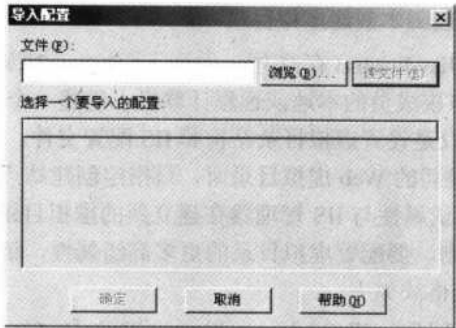


图 2-76 “导入配置”对话框

3. 使用 Windows 资源管理器创建虚拟目录

此方法仅当硬盘格式化为 NTFS 文件系统时才能使用。

(1) 在 Windows 资源管理器中，浏览要在其中创建站点虚拟目录的文件夹上单击鼠标右键，在弹出的快捷菜单中选择【共享和安全】命令，在打开的对话框中选择“Web 共享”选项卡，如图 2-77 所示。

(2) 在“共享位置”下拉列表框中选择要为之创建虚拟目录的站点，然后选择“共享文件夹”单选项，随即打开如图 2-78 所示的对话框。在“别名”文本框中键入虚拟目录的名称。在“访问权限”和“应用程序权限”两栏中设置所需的权限。具体权限说明参见本章前面的介绍。

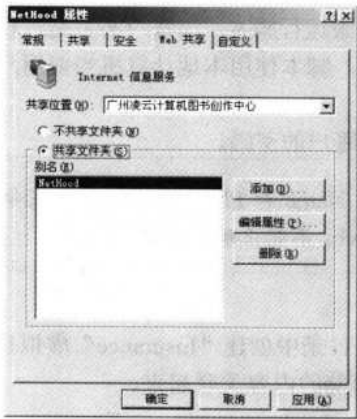


图 2-77 NTFS 文件夹属性对话框“Web 共享”选项卡

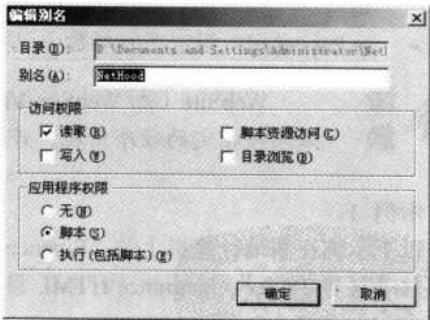


图 2-78 “编辑别名”对话框

(3) 单击【确定】按钮返回到如图 2-77 所示的对话框，再单击【确定】按钮即可完成。可以通过启动 IIS 管理器，并展开网站来检查是否已创建了虚拟目录。

在如图 2-77 所示的对话框中可以重新编辑虚拟目录属性，方法是选择相应别名的虚拟目录，然后单击【编辑属性】按钮，在打开的如图 2-78 所示的对话框中重新配置。还可删除已配置为虚拟目录的选项，方法是在如图 2-77 所示的对话框中选择相应别名选项，然后单击【删除】按钮，最后都需要单击【确定】按钮使配置生效。

96 网管员必读——网络应用（第2版）

4. 使用 Iisvdir.vbs 管理脚本创建虚拟目录

可以使用命令行脚本 Iisvdir.vbs（存储在 systemroot\System32 路径下）在运行带有 IIS 6.0 的 Windows Server 2003 家族成员的本地或远程计算机上创建一个新的 Web 虚拟目录。该命令不创建或破坏内容，而只是设置虚拟目录结构和 IIS 配置文件。

在使用 Iisvdir.vbs 创建新的 Web 虚拟目录时，只指定创建站点和标识其内容所需的基本属性。Iisvdir.vbs 使用的默认属性与 IIS 管理器在建立新的虚拟目录时使用的属性相同，并且它遵循相同的继承属性规则。要配置虚拟目录的更多高级属性，请使用 IIS 管理器。

Iisvdir.vbs 命令的语法格式如下。

Iisvdir /create WebSite[/VirtualPath] Name PhysicalPath [/s Computer [/u [Domain\]User/p Password]]

参数说明如下。

- WebSite：必需的。指定网站的描述性名称或配置数据库路径。
- VirtualPath：如有必要，指定一个指向网站内虚拟目录的路径。当虚拟目录不在网站的根目录中时，该参数是必需的。
- Name：必需的。为虚拟目录指定名称。虚拟目录名不必保持唯一，但是当网站包括同名的虚拟目录和物理目录时，在 Internet 上将看不到物理目录。
- PhysicalPath：指定驻留虚拟目录内容的物理目录。必须在本地计算机上指定一个路径，如 C:\Project\HTML。如果指定的目录不存在，Iisvdir 就会创建该目录。
- /s Computer：在指定的远程计算机上运行脚本。键入不带反斜杠的计算机名或 IP 地址。默认为本地计算机。
- /u [Domain\]User：使用指定的用户账户的权限运行脚本。该账户必须是远程计算机上 Administrators 组的成员。在默认情况下，脚本使用本地计算机当前用户的权限运行。
- /p Password：指定在/u 参数中已指定的用户账户的密码。



注意

WebSite（或 WebSite/VirtualPath）、Name 和 PhysicalPath 参数在命令行中必须按指定的顺序出现。否则，Iisvdir.vbs 不能正确地解释信息。

示例 1：

以下示例在本地计算机上的“Finance”网站的根目录中创建“Insurance”虚拟目录。它将该目录与 C:\Projects\Insurance\HTML 目录中当前存储的内容关联起来。

```
Iisvdir /create Finance Insurance c:\projects\insurance\html
```

作为响应，Iisvdir 显示以下成功消息以及新虚拟目录的基本属性。在本示例中，“Virtual Path”反映虚拟目录结构，“ROOT”表示内容所在的物理目录，“Metabase Path”表示 IIS 指定的配置数据库项。

正在连接到服务器……已完成。

Virtual Path = Finance/Insurance

ROOT = c:\projects\insurance\html

Metabase Path = W3SVC/1509060625/ROOT/Insurance

示例 2:

以下示例在远程计算机的“Finance”网站上创建“Updates”虚拟子目录。此命令使用“Finance”网站的配置数据库路径“W3SVC/1509060625”来标识该网站，并且通过在网站名称后面附加虚拟路径“Finance/Insurance”来表示。此外，该命令将“Updates”目录与远程计算机上 C:\Newstuff\Web 中存储的内容关联起来。

该示例还使用/s 参数来标识远程计算机，并使用/u 和/p 参数以用户的管理员账户权限运行 Iisvdir.vbs。

```
Iisvdir /create W3SVC/1509060625/Insurance Updates C:\Newstuff\Web /s SVR01 /u Admin01 /p p@SSw#rD2
```

作为响应，Iisvdir 显示新网站的基本属性。

正在连接到服务器……

Virtual Path = Finance/Insurance/Updates

ROOT = C:\Newstuff\Web

Metabase Path = W3SVC/1509060625/ROOT/Insurance/Updates

2.6.2 虚拟目录的配置

虚拟目录的配置与其他容器，或节点的属性配置方法一样，都是通过单击鼠标右键，在打开的快捷菜单中选择【属性】命令，在打开的属性对话框中进行配置。

因为虚拟目录是位于网站主目录以外的，通常是网站某个独立模块，所以它与网站的属性配置选项有许多相似之处，而且功能基本一样，只是作用对象不同而已。如它主要的“虚拟目录”、“文档”、“目录安全性”和“HTTP 头”4 个对话框分别如图 2-79、图 2-80、图 2-81 和图 2-82 所示，与网站属性对话框中的“网站”（参见图 2-24）、“文档”（参见图 2-32）、“目录安全性”（参见图 2-46）和“HTTP 头”对应配置选项作用和配置方法都基本一样。网站中对应的这 4 个对话框除了如图 2-82 所示的“HTTP 头”选项卡没有介绍外，其他 3 个选项卡的功能和配置方法均在本书中已介绍，在此不再赘述。

如图 2-82 所示的“HTTP 头”选项卡的配置方法与网站的“HTTP 头”选项卡配置选项和配置方法完全一样，具体将在下节介绍网站管理方法时进行。



图 2-79 虚拟目录属性对话框“虚拟目录”选项卡

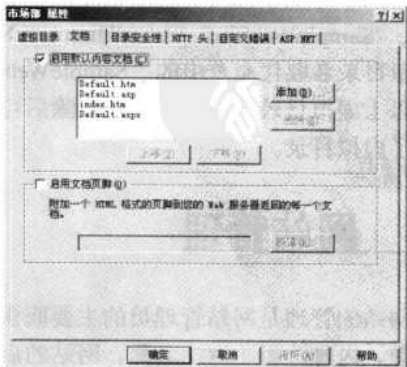


图 2-80 虚拟目录属性对话框“文档”选项卡

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

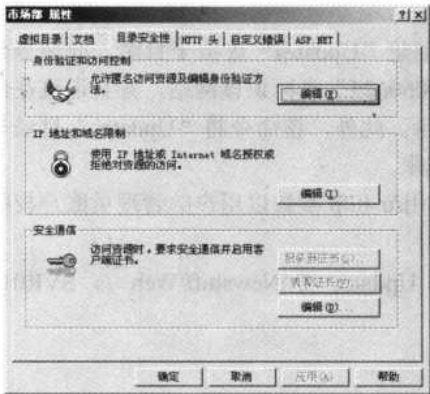


图 2-81 虚拟目录属性对话框“目录安全性”选项卡



图 2-82 虚拟目录属性对话框“HTTP 头”选项卡

2.6.3 虚拟目录的删除

虚拟目录的删除与创建一样，也可以有几种不同的方式。本节分别予以介绍。

1. 使用 IIS 管理器删除虚拟目录

在 IIS 管理器中管理虚拟目录显然是最主要的虚拟目录管理方式。具体方法是在 IIS 管理器控制台中，展开包含要删除的虚拟目录的站点，在相应虚拟目录上单击鼠标右键，在弹出的快捷菜单中选择【删除】命令，在弹出的确认框中单击【确定】按钮即可。

2. 使用 Windows 资源管理器删除虚拟目录

在 Windows 资源管理器中，浏览到包含要删除的虚拟目录的文件夹，单击鼠标右键，在弹出的快捷菜单中选择【共享和安全】命令，在打开的对话框中选择“Web 共享”选项卡，参见图 2-77 所示。然后在“别名”下拉列表框中选择要删除的虚拟目录别名，单击【删除】按钮，同样在弹出的确认对话框中单击【确定】按钮即可。

3. 使用 Iisvdir.vbs 管理脚本删除虚拟目录

注意本方法不能用于删除根虚拟目录，具体方法是在“运行”窗口中键入 `cscript iisvdir.vbs /delete "SampleWebSite" VirtualDirectoryName` 命令，当然在实际的命令中用对应的网站名称和虚拟目录名取代命令中的“SampleWebSite”和“VirtualDirectoryName”。

以上虚拟目录删除方法，在删除后可以通过启动 IIS 管理器，并展开网站来检查是否已删除了虚拟目录。

2.7 网站管理

网站的管理是网站管理员的主要职责，在 IIS 网站管理中，主要包括性能管理、服务质量管理、内容管理、网站名称、网站的启用和停止等。

2.7.1 IIS 网站管理基础

如果正在配置一个高成本的新网站，却忽然发现该站点的所有网页中都遗漏了公司的徽标；或者，试想由于技术人员忙着为计算机排除故障，你突然需要将成千上万个用户转移到另一个网站。这些棘手的日常问题已经开始说明，成功管理网站是多么的重要。尽管有效的网站管理根本上取决于管理员的能力，但还是可以使用一些基本的工具和步骤来应付普通的管理任务和突发事件。

1) 入门

首先应建立网站，同时指明哪些目录包含要发布的文档。Web 服务器无法发布未在这些指定目录中的文档。所以，配置网站第一步是确定文件的组织方式。可以使用 IIS 管理器来标识属于站点的目录。

如果希望马上开始而不创建特殊的目录结构，并且文件全部位于运行 Internet 信息服务（IIS）的计算机上的同一硬盘上，便可以立刻将 Web 文件复制到默认的主目录 LocalDrive:\InetPub\Wwwroot 来发布文档。（对于 FTP 站点，应将文件复制到 LocalDrive:\InetPub\Ftproot。）Intranet 用户能够通过下面的 URL：<http://servername/filename> 来访问这些文件。

2) 主目录

每个网站或 FTP 站点必须有一个主目录。主目录位于发布的网页的中央位置。它包含带有欢迎内容的主页或索引文件，并且包含到站点其他网页的链接。主目录映射为站点的域名或服务器名。例如，如果站点的 Internet 域名是 www.microsoft.com，而主目录是 C:\Website\Microsoft，浏览器将使用 <http://www.microsoft.com> 访问主目录中的文件。在内部网上，如果服务器名是 AcctServer，浏览器将使用 <http://acctserver> 访问主目录上的文件。

在安装 IIS 或创建新的网站时将创建默认的主目录。

3) 虚拟目录

要从主目录以外的其他目录中进行发布，就必须创建虚拟目录。虚拟目录不包含在主目录中，但在显示给客户浏览器时就像位于主目录中一样。

虚拟目录有一个“别名”或名称，供 Web 浏览器用于访问此目录。由于别名通常要比目录的路径名短，更便于用户输入。使用别名更安全，因为用户不知道文件存在于服务器上物理位置，所以便无法使用这些信息来修改文件。使用别名可以更方便地移动站点中的目录。无须更改目录的 URL，而只需更改别名与目录物理位置之间的映射。

虚拟目录和物理目录（不带别名的目录）都显示在 IIS 管理器中，滚轮图标表示虚拟目录。如图 2-83 所示说明了上述的网站示例，其中/Customers 和/PR 均为虚拟目录。

对于简单的网站，可能不需要添加虚拟目录，只需将所有文件放在该站点的主目录中即可。如果站点比较复杂或者需要为站点的不同部分指定不同的 URL，可以按需要添加虚拟目录。



图 2-83 虚拟目录示例

4) 使用重定向转发请求

当浏览器请求网站的网页时，Web 服务器将通过 URL 来定位这个网页，然后将其返回浏览器。当移动网站上的一个网页时，无法更正所有涉及到该页上的旧的 URL 的链接。要确保浏览器能够使用新的 URL 找到网页，必须通知 Web 服务器为浏览器提供新的 URL。浏览器使用新的 URL 再次请求网页。该过程称为“重定向浏览器请求”或“重定向到其他 URL”。重定向网页请求与邮政服务中的转发地址很相似，转发地址可以保证将接收地址为原居住地址的信件和邮包投递到新的居住地址。

当你更新了网站并希望其中的部分内容暂时不被用户访问，或者当你更改了虚拟目录的名称，希望使到原虚拟目录中文件的链接访问新的虚拟目录中相同的文件时，重定向 URL 非常有用。

5) 在服务器端的包含文件

通常，在 Web 内容被请求之后但返回浏览器之前动态地更改 Web 内容将十分有用。IIS 包括一个能提供此功能的，被称为在服务器端的包含文件的功能。

通过服务器端包含文件（SSI），每次得到文件请求后，便可以执行整套网站管理活动，从添加动态时间标记到运行特定的解释器命令。SSI 命令称为“指令”，在设计时被添加到网页中。当请求网页时，Web 服务器解析在网页上发现的所有指令，然后执行这些指令。通常的 SSI 指令将文件的内容插入或“包含”到网页中。例如，如果需要不断更新一个网页广告，可以使用 SSI 将广告的 HTML 源代码包含到网页中。要更新广告，仅需要修改包含广告的 HTML 源代码的文件，你无须了解使用 SSI 的脚本语言；只需遵循正确的指令语法。

6) ASP 和 ASP.NET

ASP 是服务器端脚本环境，可用来创建动态的或交互式网页并建立强大的 Web 应用程序。当应用服务器收到对 ASP 文件的请求时，它处理包含在用于构建发送给浏览器的 HTML 网页的文件中的服务器端脚本代码。除服务器端脚本代码外，ASP 文件也可以包含 HTML（包括相关的客户端脚本）和 COM 组件调用，上面谈及的这些组件可执行不同任务，如连接到数据库或处理商业规则。ASP 要求使用一种脚本语言，如 VBScript 或 JScript。

ASP.NET 是新一代的 Microsoft 服务器端脚本环境。它提供一种新的编程模式和结构，使 Web 开发者能够构建和部署比以前更安全、更灵活、更稳定的企业类 Web 应用程序。

2.7.2 网站性能管理

对 Web 服务器进行性能调整既是一门学问，又是一门艺术。在确定什么设置和硬件最适合网站要求时，进行反复试验是必要的。在开始评估 Web 服务器的性能之前，最好先制订一份计划。了解应用程序或网站的基本概况，以及它们在不同条件下的表现也同样重要。

制订性能调整计划的第一步是建立一个受控制的环境，以便在其中对网站进行测试，对预计负载进行性能分析，并在该受控制的环境中测试性能，然后才能将 Web 服务器放到 Internet 上。根据不同的时段中界面请求数量的不同，服务器的性能也会大有不同，因此一定要在若干不同的负载下监视被测试站点，以获得服务器的真实的活动信息。

要改善服务器性能，请检查系统的各个部分，以找出潜在的瓶颈，包括自定义应用程序、内存、CPU、网络、硬盘，以及与后端服务器和数据库的连接。如果 IIS 或 Windows 中的硬件或软件设置的配置不当，也会导致瓶颈。一份好的监视计划将检查 Web 服务器系统的各个部分的性能。

在确定服务器的性能统计信息之后，可以通过启用后面的主题中列出的一些服务质量功能或通过配置数据库和注册表设置进行更改来改善性能。启用功能并对配置数据库或注册表进行更改时应一次一个地进行，并使用经过测试的还原计划。如果同时进行了多个更改，则很难评估单个更改对性能的影响。进行每个更改之后，请继续监视服务器，以了解该更改是否产生了预期的效果。如果产生了不需要的效果，则请将服务器还原到其以前的状态。进行更改之后，请监视资源（如内存、CPU 和硬盘）的性能。对一个设置的调整可能会在系统的其他部分产生瓶颈。在评估了一个更改的影响之后，请确定是否还需要进行其他更改。

1. 性能 and 安全性

在性能与用户对于 Web 应用程序的安全性的顾虑之间找到平衡点是你面临的最重要的问题之一，特别是在运行电子商务网站的情况下。安全的 Web 通信比不安全的 Web 通信需要更多的资源，因此了解何时应使用何种安全技术（如安全套接字层（SSL）协议、证书或各种 Windows 身份验证方法）是很重要的。例如，主页或搜索结果界面很有可能不需要通过 SSL 运行。然而，你需要确保结账或购物界面是安全的。

如果使用 SSL，要意识到，建立初始连接需要的时间比使用 SSL 会话缓存中的安全信息重新进行连接需要的时间长 5 倍。在 Windows 2000 和更高版本中，SSL 会话缓存的默认超时已经更改为 5 分钟。在此数据从缓存中删除或“清空”之后，客户端和服务器必须建立全新的连接。

如果你计划将支持较长的 SSL 会话，请考虑使用 Server Cache Time 注册表设置延长超时设置。如果你预计会有成千上万的用户使用 SSL 连接到你的站点，则更安全的方法是估计 SSL 会话会持续多长时间，然后将 ServerCacheTime 参数设置得比估计的值稍长一些，请不要将超时值设置得比此值长太多，因为这样服务器可能会将陈旧的数据保留在缓存中。此外，要确保启用保持 HTTP 连接（默认情况下是启用的）。SSL 会话在与“保持 HTTP 连接”复选项（参见图 2-24 所示）一起使用时不会过期，除非浏览器明确地关闭连接。

Windows Server 2003 家族和 Internet 信息服务 IIS 6.0 安全服务已集成到许多操作系统服务中。这意味着无法从这些服务的其他方面单独监视安全功能。相反，测量安全开销的最常

102 网管员必读——网络应用（第2版）

见方法是，在使用安全功能和不使用安全功能的情况下进行测试，以便比较两种情况下的服务器性能。测试应该在使用固定工作负载和固定服务器配置的情况下进行，这样，安全功能就是唯一的变量。在测试过程中，请测量以下计数器。

- **Processor Activity and the Processor Queue:** 诸如身份验证、证书、安全套接字层(SSL)和加密等安全功能需要进行大量的处理，因此应在使用这些安全功能与性能目标之间找到平衡点。

你可能会在特权模式和用户模式下看到增多的处理器活动，并且也会看到上下文切换和中断的频率增多。如果服务器中的处理器无法处理大量的负载，则很有可能会产生队列。使用自定义硬件（如用于进行加密的加密加速器）可能会有所帮助。当你通过使用证书向导创建证书时，可以选择使用加密加速器的加密服务提供程序。请注意，如果使用了 SSL 协议，Lsass.exe 可能会占用大量的 CPU 时间，因为 SSL 处理是在 Lsass.exe 进程中进行的。

- **Memory:** 安全性要求系统必须存储和检索更多的用户信息。
- **Network Traffic:** 你还可能会看到 IIS 服务器和用于对登录密码进行身份验证和验证 IP 地址的域控制器之间的通信量变大。
- **Latency and Delays:** 由于复杂的安全功能（如 SSL）产生的最明显的性能下降是加密与解密（这两个过程都使用大量的处理器周期）所占用的时间和资源。从使用 SSL 协议的服务器中下载文件会比从不使用 SSL 的服务器中下载文件慢 10 到 100 倍。



注意

如果服务器既运行 IIS 又作为域控制器，那么域服务所消耗的处理器时间、内存、网络 and 磁盘活动的比例可能会大大地提高。增多的活动足以阻止 IIS 服务有效地运行。强烈建议你不要在域控制器上运行通信量很高的 Web 服务器。

2. 网站性能设置

可以通过调整 Internet 信息服务 (IIS) 配置数据库属性和注册表项来调整 Web 服务器的性能。提高或降低设置值常常可以缓解瓶颈和改善性能，但对配置数据库或注册表的更改也可能在服务器环境的其他部分产生瓶颈。在对服务器环境进行更改之前或之后都要对性能进行监视，以确定更改是否有益。

此处所介绍的仅适合于 Web 服务器性能的配置数据库和注册表设置的建议值。



警告

使用注册表编辑器不当可能导致需要重新安装操作系统的严重问题。因为注册表编辑器会跳过标准安全保护（禁止你输入存在冲突或者有可能降低性能或损坏系统的设置），所以在更改注册表时一定要格外小心。

对于性能问题，在对注册表进行更改之前，请先尝试更改配置数据库和缓存的设置。要对 Windows 和 IIS 进行配置或自定义，只要有可能，请使用控制面板或 Microsoft 管理控制台 (MMC) 中的程序。

1) 配置数据库的设置

表 2-16 列出了对于调整 Web 服务器最重要的配置数据库属性。可以通过使用 Windows Management Instrumentation (WMI) 或通过使用文本编辑器直接对配置数据库（位于 systemroot\System32\Inetsrv 文件夹下的 MetaBase.xml）进行编辑来检索和更改这些属性，如图 2-84 所示。对这些属性中大多数属性的更改在重新启动万维网发布服务 (WWW 服务) 之前不会生效。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 2-84 打开的配置数据库文件

表 2-16 可调整 Web 服务器性能的配置数据库选项

配置数据库属性	描 述
AppAllowDebugging	指定在服务器上是否启用 ASP 调试。在启用此属性的情况下，IIS 应用程序线程是序列化的；对于每个应用程序，一次只允许执行一个线程。序列化线程会对 Web 服务器性能产生负面影响。建议在所有产品服务器上将此属性设置为 false
AspBufferingOn	允许将应用程序的所有输出收集在 ASP 输出缓冲区中，然后再将缓冲的信息刷新到客户端浏览器（默认行为）。如果将此属性设置为 false，那么在客户端浏览器可用时 ASP 脚本的输出将被写入到客户端浏览器。建议在所有产品服务器上将此属性设置为 true
AspQueueConnectionTestTime	确保 IIS 不将时间浪费在处理用户已放弃的请求上。此设置会显著地改善 Web 应用程序的性能。如果某一请求在队列中的时间长于队列连接测试时间，那么服务器将在开始执行之前检查客户端是否仍处于连接状态 此功能用于处理急躁的用户用在同一界面上的很多请求尝试填满请求队列的问题。应将该值设置得小一些，例如，3 秒。是否更改此值要依据服务器运行的 Web 应用程序的类型来决定。长时间运行的 ASP 界面也可以使用 Response.IsClientConnected 方法检查客户端是否仍在等待界面的其余部分。长时间运行的界面应使用 Response.Flush 确保用户觉察到界面仍在连接中并且在进行高效的处理
AspRequestQueueMax	指定允许进入队列的并发 ASP 请求的最大数量。此设置的效果取决于应用程序的行为。如果请求的执行时间非常短，且在队列中的时间非常短，那么提高默认值的限度是合理的
AspScriptEngineCacheMax	指定 ASP 页缓存在内存中的脚本引擎的最大数量。根据应用程序中的内容的类型调整默认值。（默认值不包括当前正在运行的脚本引擎）如果有成千上万的不同页，你会体验到提高缓存大小的一些好处：大多数频繁请求的网页都可以轻松地访问到。脚本引擎缓存的好处意味着你无须将模板重新编译为字节代码
AspScriptFileCacheSize	指定存储在 ASP 模板缓存中的预编译脚本文件的数量。如果设置为 0，则不缓存任何脚本文件。如果设置为-1，则缓存所有被请求的脚本文件。如果你有许多不同的 ASP 页，则可以增大默认值。不要将此属性的值设置为 0。如果值为 0，则会关闭所有 ASP 缓存，会严重影响服务器的性能

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(续表)	
配置数据库属性	描 述
AspSessionMax 和 AspSessionTimeout	AspSessionMax：指定 IIS 允许的并发会话的最大数量 AspSessionTimeout：指定在发出与对象关联的最后一个请求之后会话对象保持的默认时间长短（以分钟为单位） 对于利用会话的应用程序，缩短会话超时时间以减少服务器所需要的开销可能是明智的做法。然而，如果并发会话的比例很大，则可能有必要使用最大的会话超时值
AspProcessorThreadMax	指定 IIS 为每个处理器创建的工作线程的最大数量。IIS 所允许的每个 ASP 进程的工作线程的最大数量是 AspProcessorThreadMax 乘以服务器上处理器的数量。可以降低此值然后监视性能。如果性能降低，请恢复 AspProcessorThreadMax 原来的值
AspTrackThreadingModel	指定 IIS 是否检查应用程序实例化的所有组件的线程模型。不建议启用此属性。如果将此配置数据库属性设置为 false，即可避免 ASP 线程模型跟踪所产生的开销，并且你可能会看到 ASP 应用程序的性能改善。然而，如果将此属性设置为 true，你计划给予应用程序作用域的所有组件都必须是灵活的；换句话说，要么被标记为双线程的，并聚集自由线程的封送器，要么被标记为 ThreadingModel=Neutral 如果应用程序作用域内的组件不是灵活的，那么当你尝试实例化组件时 ASP 就会产生错误。此外，如果此属性为 false，那么缺乏 OnStartPage 或 OnEndPage 方法并在 ASP 应用程序中被实例化的所有对象都比它们在相反的情况下更早地释放。这样就应能够改善应用程序的可扩展性
CacheISAPI	指出 Internet 服务器 API (ISAPI) 扩展在使用之后是否在内存中缓存。如果此属性的值是 true，那么 DLL 文件在服务器停止之前会保留在缓存中；如果该值是 false，那么在扩展 DLL 不再使用之后将从内存中卸载 ISAPI 扩展。ISAPI 扩展是缓存还是不缓存，取决于在它们加载到内存供使用时此属性的值。因此，如果此属性在扩展被加载并缓存之后被更改，那么更改不会影响该扩展 将此属性设置为 false 对于调试很有帮助，但建议你在所有产品 Web 服务器上将此值设置为 true。为每个请求重新加载 ISAPI 扩展 DLL 文件会降低性能。ASP.dll 本身就是一个 ISAPI 扩展，因此禁用此属性也会降低 ASP 性能

2) 注册表设置

此部分列出了在调整 Web 服务器时应考虑的注册表项。每个列出的注册表项都包括驻留相同位置的设置的注册表路径，并包括名称、范围、默认值和每个设置的作用的描述。需要重新启动 IIS 才能使新的 WWW 服务设置生效。

DisableMemoryCache

注册表路径: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters

数据类型: REG_DWORD

默认值: 0 (已禁用)

范围: 0~1

DisableMemoryCache 禁用服务器缓存。要确保在所有产品服务器上将此参数设置为 0。如果将此参数设置为 1，那么就会禁用静态文件缓存。尽管禁用缓存可能会对调试有用，但这样做会严重降低产品服务器的性能。此参数无法使用 IIS 管理器进行配置

MaxCachedFileSize

注册表路径: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters

数据类型: REG_DWORD

默认值: 256KB (262144bytes)

第2章 IIS 6.0 Web 网站配置与管理 105

MaxCachedFileSize 确定可以放在缓存中的文件的最大大小。IIS 不缓存大于 **MaxCachedFileSize** 字节的文件。如果你正在运行专用的大型 Web 服务器，可能需要将此值添加到注册表中，以提高缓存中可以保存的文件大小

MemCacheSize

注册表路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters

数据类型：REG_DWORD

默认值：大约为可用物理内存的一半，以兆字节为单位

范围：0~2500MB

MemCacheSize 指定 IIS 用来作为其文件缓存的内存的最大量。如果 IIS 不需要这么多内存，可以留给其他应用程序使用。如果注册表中没有此值，IIS 用做缓存的量不超过 Web 服务器上可用内存的一半（是每隔 60 秒动态地计算出来的）。如果你正在运行专用的大型 Web 服务器，可能需要将此值添加到注册表中，以提高 IIS 可以使用的内存量。当你将此对象添加到注册表时，必须以兆字节为单位指定此大小

ObjectCacheTTL

注册表路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters

数据类型：REG_DWORD

默认值：30（秒）

范围：0~4294967295（无限制）

ObjectCacheTTL 控制静态文件缓存的生存时间（TTL）设置，该设置定义对象（包括文件）存放在缓存中的时间长短。如果内存缓存中的对象在所定义的时段内未被引用，则该对象将被清除出缓存。默认情况下，此值未包括在注册表中。如果你希望更改此默认值，则必须手动添加。如果系统内存有限，或者服务器内容是动态的，你可以使用一个较低的 TTL 来防止系统内存被用于缓存大量动态的对象。将值设置为 0xFFFFFFFF 将禁用对象缓存清理程序并允许缓存对象保留在缓存中，直到它们被覆盖为止。如果服务器有足够的系统内存而且数据是相对稳定的，则禁用缓存清理程序将很有用。其他站点可以选择折中，将此值提高到几分钟

PoolThreadLimit

注册表路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters

数据类型：REG_DWORD

默认值：2*#MB

范围：0~4294967295（无限制）

PoolThreadLimit 指定可以在 **Inetinfo.exe** 进程中创建的 I/O 工作线程的最大数量，该设置将限制同时连接的数量。IIS 将 **PoolThreadLimit** 设置为计算机中当前 RAM 的兆字节数量的两倍。如果此值大于 256，则使用 256。如果注册表中已经有该值，那么它就会覆盖 IIS 的计算值。每个池线程都监视网络请求并对其进行处理，处理方法是，发回静态文件或者将该请求传递到 ISAPI 扩展 DLL（如 ASP）或传递到通用网关接口（CGI）。如果 ISAPI 扩展同步对请求进行处理，它将需要花很长时间来处理请求，而且会占用工作线程，这样 IIS 处理其他请求的工作线程数会变少。因此，高质量编码的 ISAPI 扩展（如 ASP）实现它们自己的线程池，将请求放在队列中，并使用其自己的线程异步对请求进行处理，这样就不会占用 IIS 工作线程了。一般来说，如果发现默认限度 256 个线程不够，那么 ISAPI 扩展的编码质量可能较差，占用了 IIS 工作线程。

PoolThreadLimit 是包括所有 IIS 工作线程（包括 HTTP、FTP、NNTP 和 SMTP 服务）的硬性限制。**PoolThreadLimit** 总是大于或等于 **MaxPoolThreads**。

ASP 线程池是单独的一组线程。其大小受 **AspProcessorThreadMax** 配置数据库设置的控制。未处理的 ASP 请求的最大数量是 **AspRequestQueueMax** 和 **AspProcessorThreadMax** 的总和。

PoolThreadLimit 是包含所有 IIS 线程的硬性限制，它始终大于或等于 **MaxPoolThreads**

106 网管员必读——网络应用（第2版）

MaxPoolThreads

注册表路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\inetInfo\Parameters

数据类型：REG_DWORD

默认值：4

范围：0~4294967295（无限制）

MaxPoolThreads 指定为每个处理器创建的 I/O 工作线程的数量。每个池线程都监视网络请求并对其进行处理。MaxPoolThreads 计数不包括 ISAPI 应用程序使用的线程；它只表示可用于处理静态文件请求的工作线程数量。IIS 将按需要创建更多线程，以处理 ISAPI 请求。IIS 工作线程的总数不得大于 PoolThreadLimit。

默认情况下，只能同时运行 4 个 CGI 应用程序。如果运行多个 CGI 应用程序，应该增加该值以提高吞吐率。可以将 UsePoolThreadForCGI 的值（在.\Services\W3SVC\Parameters 下）设置为 false（或 0），但这有点危险，因为在大量使用 CGI 应用程序时性能会明显降低。通常，每个处理器最好不要创建超过 20 个线程。

ListenBackLog

注册表路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\inetInfo\Parameters

数据类型：REG_DWORD

默认值：15

范围：1~250

ListenBackLog 指定在队列中允许的等待服务器处理的活动的最大数量。通常没有必要使用或修改此项，虽然在频繁使用的情况下将此值最多提高到 300 会非常有益。

2.7.3 网站服务质量管理

服务质量（QoS）包括了服务机构实施的、用来保持特定质量水平的一组方法或过程。在 Windows 环境中，QoS 是一组服务要求，网络必须满足这些要求才能确保适当服务级别的数据传输。QoS 的目的是确保特定站点或应用程序不会独占服务器资源，如内存或 CPU 周期。QoS 可帮助管理员控制 Internet 信息服务（IIS）使用资源的方式，如站点、应用程序池或整个万维网发布服务（WWW 服务）。

本节包括下列信息。

- 限制连接：介绍如何设置 Web 服务器允许的连接数量限制。
- 设置连接超时：介绍如何在 Web 服务器上设置连接超时值。
- 使用 HTTP 压缩：介绍 HTTP 压缩及它可如何改善带宽利用率。
- 限制带宽：介绍如何更改 Web 服务器和个人网站使用的带宽。
- 保持 HTTP 连接：介绍如何使用保持 HTTP 连接请求以保持打开的连接。
- 启用 CPU 监视：介绍如何监视并中止有问题的应用程序。
- 配置应用程序池队列长度限制：介绍如何限制 IIS 在任何应用程序池队列中保存的请求的数量，以便请求的数量不会增加到耗尽服务器资源的程度。

1. 限制连接和带宽

1) 限制连接

限制连接可限制网站和 Web 服务器上同时连接的数量。如果连接的数量达到指定的最大值，以后所有的连接尝试都会返回一个错误信息，然后连接被断开。

限制连接是为其他用途保留带宽的一种方法，这些用途包括电子邮件服务器、新闻服务

器或运行于同一安装位置的其他网站等。限制连接还可以保留内存，并防止意图用大量客户端请求造成 Web 服务器超载的恶意攻击。

要判断是否应该限制连接，请使用系统监视器来记录“WWW 服务”和“FTP 服务”对象中的当前连接、最大连接数和连接尝试总数计数器。继续记录一段时间，直到完全把握常规范围；通常，这可能几天到一周或更长的时间，而且需要定期重复执行。

既可以为所有网站和 FTP 站点建立全局 WWW 服务或 FTP 服务连接限制，也可以为单个网站或 FTP 站点建立连接限制。IIS 在检查为单个站点设置的连接限制之前，会检查全局连接限制。如果超出了全局连接限制，则无论为单个站点设置的连接限制是什么，IIS 都会返回错误 403.9（禁止用户过多）。你可以在 IIS 5.0 中自定义连接限制错误，而在 IIS 6.0 中则不允许自定义此错误。

“不受限制”连接选项允许任意数量的同时连接，只要你的网络带宽和处理器支持。注意，允许对 Web 服务器无数量限制的同时连接会给服务器上的所有站点带来遭受恶意攻击的危险，这种攻击的手法是让数以千计的客户端连接到该服务器，大量消耗内存和带宽资源，延迟后续服务。

2) 限制带宽

如果 Web 服务器使用的网络或 Internet 连接也被其他服务使用，例如电子邮件或新闻，可能希望限制 Web 服务器所使用的带宽，以便其他服务也可使用。如果 Web 服务器作为多个网站的宿主，你可以单独控制每个站点使用的带宽。

带宽限制使用数据包计划程序来管理何时发送数据包。当你用 IIS 管理器来配置某个站点使用带宽限制时，会自动安装数据包计划程序，而且 IIS 会自动将带宽限制设置为最小 1024 字节/秒。但是，如果使用其他方法（例如 Active Directory 服务界面（ADSI）或 Windows Management Instrumentation（WMI）），则必须安装数据包计划程序，使带宽限制能正常工作。



注意

使用 ADSI 或 WMI 来配置带宽限制时，必须将带宽限制设置为大于或等于 1024 字节/秒，因为数据包计划程序无法执行低于 1024 字节/秒的带宽限制设置。单个站点或整个万维网都不使用数据包计划程序时，应卸载该应用程序。

启用带宽限制之前，请使用系统监视器检查“网络接口”对象中的总字节数/秒或当前带宽计数器。如果希望比较传入和传出流量，请检查发送的字节数/秒和接收的字节数/秒。

还要比较“网络接口”对象的值和你的网络连接的总带宽。对于“正常”的负载，服务器使用的带宽不应超过其全部可用带宽的 50%。如果服务器有较大的高峰负载，请将正常负载保持在 50% 以下。剩下的带宽可在高峰期时使用。

如果服务器或特定站点一直使用的带宽超过可用带宽的 50%，请使用本节后面介绍的方法来限制带宽。但设置全局 WWW 服务最大带宽不会替代已为服务器上的单个网站建立的最大带宽。单个站点根据已设置的最大值来限制带宽，而全局设置限制所有其他未限制带宽的网站。

设置网站 WWW 服务连接限制和带宽限制的方法如下。

（1）在 IIS 管理器中，展开本地计算机，在“网站”文件夹（设置对 IIS 管理器中所有网站都生效）或相应的网站（设置仅对相应网站生效）文件夹上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“性能”选项卡，如图 2-85 所示。

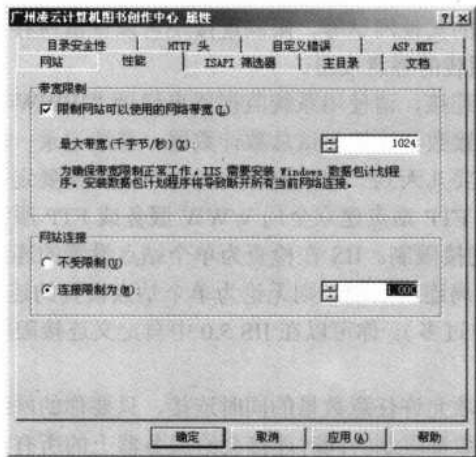


图 2-85 网站属性对话框“性能”选项卡

(2) 选择“限制网站可以使用的网络带宽”复选项，然后在下面的“最大带宽”（千字节/秒）滚动列表框中键入一个限制的带宽值，默认为 1Mbps。具体要根据实际可用的网络带宽和欲分配的最大带宽值而定。在“网站连接”栏中选择“连接限制为”单选项，然后在后面的滚动列表框中键入在 Web 服务器上允许的同时连接的最大数量。默认为 1000 并发给用户。

(3) 单击【应用】按钮，然后单击【确定】按钮完成配置。

2. 设置连接超时和保持 HTTP 连接

1) 设置连接超时

连接超时有助于减少由空闲连接消耗的处理资源损失。启用连接超时，IIS 会在连接级别执行以下类型的连接超时。

- 客户端已向服务器发送了数据，现处于空闲状态造成的连接超时。
- 已建立了与服务器的连接，但客户端未发送数据时造成的服务器侦听超时。
- 响应超时（基于可配置的最小字节数/秒的值）。
- 请求超时，它禁止客户端向服务器发送不合理的慢速请求（例如，1 比特/秒）。

要判断是否应该设置连接超时，请使用系统监视器记录万维网发布服务（WWW 服务）和 FTP 服务对象中的当前连接、最大连接和连接尝试总次数计数器。继续记录一段时间，直到完全把握常规范围；通常，这可能需要几天到一周或更长的时间，而且需要定期重复执行。



在 IIS 6.0 中，ServerListenTimeout 配置数据库属性不再存在，它已被以下配置数据库属性代替：

ConnectionTimeout: 指定服务器断开非活动的连接前要等待的总时间数（以秒为单位）。

MinFileBytesPerSec: 当 IIS 响应客户端请求时，MinFileBytesPerSec 属性决定了客户端接收整个响应的长短。如果客户机接收整个响应所花的时间太长，内核模式驱动程序 HTTP.sys 会根据超时值终止连接。超时值的计算方式是：将整个响应（包括标题）的大小除以 MinFileBytesPerSec 属性，获得最大的允许响应时间长短（以秒为单位）。例如，如果将 MinFileBytesPerSec 设

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

置配置为 2048, 那么大小为 2KB 的响应需要在 1 秒内完成。默认值是 240 字节/秒。此时间段可防止客户机发送较大的响应请求 (比如文件下载), 然后故意以较慢的速度接收响应, 消耗服务器上的资源, 甚至有可能中断为其他客户机提供的服务。

2) 保持 HTTP 连接

大多数 Web 浏览器要求服务器在多个请求中保持连接打开。这被称为保持 HTTP 连接。保持连接是一个 HTTP 规范，它能够显著增强服务器性能。如果没有它，浏览器将必须为包含多个元素（如图形）的页进行大量的连接请求。可能需要为每个元素进行单独连接。这些额外的请求和连接要求额外的服务器活动和资源，这将会降低服务器的效率。它们还会大大降低浏览器的速度和响应能力，尤其是在网络连接速度较慢的地方。

在安装进程中，将默认启用保持 HTTP 连接。启用后，保持连接的持续时间是连接超时设置允许的时间。

集成安全性和基于连接的验证服务需要保持 HTTP 连接。匿名身份验证（使用 NTLM）需要保持 HTTP 连接。使用匿名身份验证禁止网站保持 HTTP 连接会使对该网站的请求失败。

设置 WWW 服务连接超时和保持 HTTP 连接的具体方法如下。

(1) 在 IIS 管理器中, 展开本地计算机, 在“网站”文件夹(设置对 IIS 管理器中所有的网站都生效)或相应的网站(设置仅对相应网站生效)文件夹上单击鼠标右键, 在弹出的快捷菜单中选择【属性】命令, 在打开的对话框中选择“网站”选项卡, 如图 2-86 所示。在“连接超时”文本框中, 键入 IIS 在重置空闲连接之前保持该连接的最大秒数。默认为 120 秒。



图 2-86 网站属性对话框“网站”选项卡

(2) 确保已选中了“保持 HTTP 连接”复选项。单击【应用】按钮，然后单击【确定】按钮完成配置。

110 网管员必读——网络应用（第2版）

3. 使用 HTTP 压缩

如果你的站点使用了很大的带宽，或者你希望更加有效地使用带宽，请考虑启用 HTTP 压缩。HTTP 压缩在启用压缩的浏览器和 IIS 之间提供了更短的传输时间。既可以只压缩静态文件，又可以同时压缩静态文件和应用程序响应。如果网络带宽受到限制，使用 HTTP 压缩会很有用（至少对于静态文件来说），除非处理器利用率已经很高。

动态处理会影响 CPU 资源。对动态响应启用压缩后，每次请求动态响应时都会进行压缩。这意味着并不缓存动态响应，每次请求动态响应时，服务器可能需要更多的 CPU 周期来压缩和发送响应。已压缩的静态响应可以被缓存，因此不会像动态响应那样影响 CPU 资源。

1) HTTP 压缩的工作原理

IIS 在接收到请求时，将检查浏览器是否允许压缩。然后 IIS 会检查文件扩展名，以确定请求的文件是否为静态文件或包含动态内容。如果文件包含静态内容，IIS 将查看以前是否请求过该文件并且已将该文件以压缩格式存储在临时压缩目录中。如果文件没有以压缩格式存储，IIS 会将未压缩的文件发送到浏览器，并在临时压缩目录中添加此文件的压缩副本。如果文件以压缩格式存储，IIS 会将压缩过的文件发送给浏览器。在浏览器首次请求之前，所有文件都不压缩。

如果文件包含动态内容，IIS 将在生成此响应时进行压缩并将压缩后的响应发送给浏览器。不存储此文件的副本。

压缩静态文件的性能代价较小，而且通常只压缩一次，因为该文件随后被存储在临时压缩目录中。压缩动态生成的文件的代价要高一些，因为它们并不存储，并且每次请求时都必须重新生成。在浏览器上展开文件的代价非常小。压缩文件的下载速度更快，所以对于提高使用有限带宽的网络连接（如调制解调器连接）的所有浏览器的性能特别有好处。

在默认情况下，压缩文件的截止日期是 1997 年 1 月 1 日，以防止代理服务器将缓存的压缩文件副本发送到未启用压缩的浏览器。这也意味着浏览器在下次用户请求时并不显示文件的缓存副本，而是返回服务器请求新副本。

2) 启用 HTTP 压缩

如果服务器生成大量的动态内容，则需要考虑压缩造成的额外处理代价是否值得付出。如果 % 处理器时间计数器已经达到或超过 80%，则不建议启用 HTTP 压缩。

要创建一个基线，请使用系统监视器记录几天内“处理器”对象的 % 处理器时间计数器的值。此计数器有一个总实例以及系统中每个处理器的单独实例（如果服务器有多个处理器，应该同时观察单个处理器和总的处理器情况，以发现工作量分配不平衡之处）。此外，还应该记录“网络接口”对象的发送的字节数/秒计数器。

启用压缩并继续在一段时间内记录这些计数器的值，最好是几天，这样就能得到好的对比依据。然后将未压缩时的值和压缩过的值相比较。



如果在测试期间看到阻塞或瓶颈现象，应立即停止测试。任意一个计数器的值明显下降都意味着与未启用压缩时相比，启用压缩已降低了性能。

启用 HTTP 压缩的步骤如下。

- (1) 在 IIS 管理器中，展开本地计算机，在“网站”文件夹（在此不能针对具体网站设

置)上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“服务”选项卡，如图 2-87 所示。

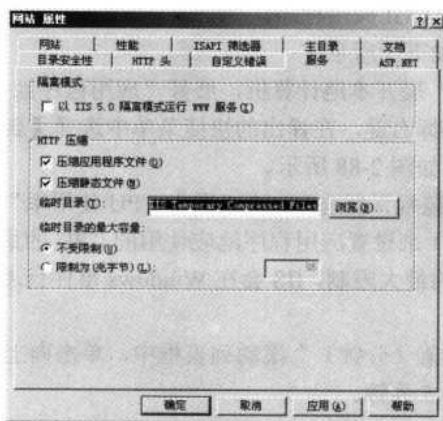


图 2-87 网站属性对话框“服务”选项卡

(2) 在“HTTP 压缩”栏中选择“压缩应用程序文件”复选项，以压缩应用程序文件；选择“压缩静态文件”复选项，可以只压缩要传送给启用压缩的客户端的静态文件。

在“临时目录”文本框中，输入某个本地目录的路径，或者单击【浏览】按钮来查找目录。压缩文件保存在这个临时目录中。该目录必须在 NTFS 分区的本地驱动器上。该目录不能是压缩目录，而且不能被共享。

在【临时目录的最大容量】栏中，如果选择“限制为（兆字节）”单选项，并在它旁边的文本框中输入数值，IIS 会在达到设置的限制时根据“最近最少使用”原则自动清理临时目录；如果选择“不限制”，则压缩文件的临时目录所占容量不作限制，只受磁盘空间限制。

(3) 单击【应用】按钮，然后单击【确定】按钮完成配置。

4. 启用 CPU 监视

CPU 监视是一个工具，它监视并自动关闭消耗大量 CPU 时间的工作进程。CPU 监视是为单个应用程序池而启用的。管理员可以对应用程序池设置以下两种 CPU 监视操作。

- 错误事件日志记录：当特定应用程序池或应用程序池组的 CPU 使用率达到设定的限制时，IIS 在 Windows 事件日志中记录一个错误。错误中包含特定工作进程和超出 CPU 限制的应用程序池的名称。使用 IIS 管理器启用 CPU 监视时，会显示为“无操作”。
- 停止有问题的应用程序：IIS 将错误写入到 Windows 事件日志中之后，它会向每个工作进程发出应用程序池的 ShutdownTimeLimit 设置的多少秒后关闭命令，开始关闭应用程序池中的所有工作进程。如果到时间后进程仍未关闭，只要 IIS 未配置为替换工作进程或工作进程没有调试配置，那么 IIS 会终止工作进程。应用程序池关闭，而且在 CPUResetInterval 时间窗口到期之前会一直关闭。一旦 CPUResetInterval 时间窗口到期，应用程序池便会重新启动。使用 IIS 管理器启用 CPU 监视时，会显示为“关闭”。

在启用 CPU 监视之前，请注意以下事项。

- IIS 必须以工作进程隔离模式工作。
- CPU 监视只适用于应用程序池。
- CPU 监视不适用于 CGI 应用程序。

启用 CPU 监视的步骤如下面所示。

(1) 在 IIS 管理器中，展开本地计算机，展开“应用程序池”文件夹，在要启用 CPU 记账的应用程序池上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“性能”选项卡，如图 2-88 所示。

(2) 选择“启用 CPU 监视”复选项。在“最大 CPU 使用率”滚动列表框中，单击向上和向下箭头（也可直接输入）来设置应用程序池应使用的 CPU 的最大百分比。如果应用程序池的 CPU 使用率超出指定的最大限制，IIS 会在 Windows 事件日志中生成一条错误信息。默认为 100%。

在“刷新 CPU 使用率值（分钟）”滚动列表框中，单击向上和向下箭头（也可直接输入）来设置刷新率。默认为 5 分钟。

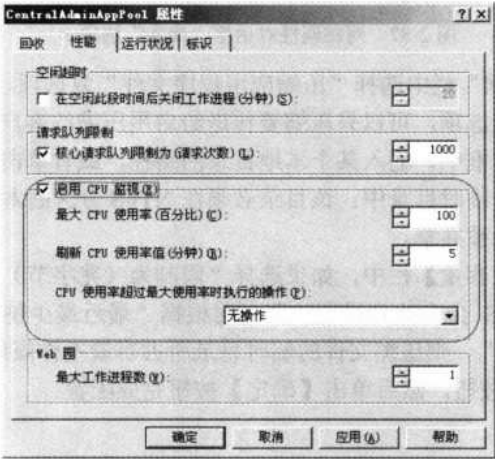


图 2-88 应用程序池属性对话框“性能”选项卡

在“CPU 使用率超过最大使用率时执行的操作”下拉列表框中，为指定的应用程序池选择所需的操作。如果选择“无操作”选项，则可使 IIS 在指定的应用程序池达到最大 CPU 使用率限制时，在 Windows 事件日志中生成一条错误信息。

(3) 单击【应用】按钮，然后单击【确定】按钮完成配置。

5. 配置应用程序池队列长度限制

应用程序池队列长度限制可防止大量请求排队等候，造成服务器超载。当启用应用程序池队列长度限制时，IIS 在将新请求加入队列前，先监视指定的应用程序池队列中的请求数量。如果将新的请求添加到该队列时，超出了队列的大小限制，服务器会拒绝该请求，并向客户端发送一个 503 错误响应（不能自定义该响应）。然而，即使你将队列长度限制改为小于当前队列长度的值，队列中已有的请求仍会留在队列中。

更改应用程序池队列长度限制的步骤如下。

(1) 在 IIS 管理器中，展开本地计算机，展开“应用程序池”文件夹，在要启用 CPU

记账的应用程序池上单击鼠标右键，在弹出菜单中选择【属性】命令，在打开的对话框中选择“性能”选项卡，参见图 2-88 所示。

(2) 在“请求队列限制”栏中选择“核心请求队列限制为”复选项，然后在“请求次数”滚动列表框中单击向上和向下箭头（也可直接输入）设置队列中请求的最大数目。默认为 1000 次。

(3) 单击【应用】按钮，然后单击【确定】按钮。



如果未选中“核心请求队列限制为”复选项，IIS 将不会执行队列限制。由于不限制队列中的请求数量，IIS 可能会将请求一直添加到队列中，直到服务器的内存耗尽为止。

2.7.4 网站的其他管理

网站的其他管理包括：网站名称管理、网站内容管理、网站访问限制、MIME 类型支持和网站的启用与停止等方面。下面分别予以介绍。

1. 网站名称管理

运行 IIS 的服务器可以主控多个网站。可以说，每个网站都运行在一个虚拟服务器上。每个虚拟网站都有一个描述性名称，并支持一个或多个主机头名称。主机头名称使得在一台计算机上主控多个域名成为可能。

2. 启用和停止网站

启用和停止网站的方法很简单，只需在正在运行的网站上单击鼠标右键，在弹出的快捷菜单中选择【停止】命令，则可以把正在运行的网站停止；如果相应网站当前正处于停止状态，在其上单击鼠标右键，在弹出的快捷菜单中选择【启动】命令，则可以把正处于停止状态的网站重新启用。

3. 网站内容管理

网站的内容管理包括网站内容的过期管理和分级管理两个主要方面。

如果网站中有时间敏感信息，可以配置设置来保证过期信息不被代理服务器或 Web 浏览器缓存。你可以配置网站内容，使之在任何的时间自动过期。当启用内容过期时，Web 浏览器将比较当前日期和截止日期，以便决定是显示缓存页还是从服务器请求更新的页。ASP.NET 这样的服务器端技术可用于动态更改提供的内容。通常，时间敏感信息只限于单个文件、目录或网站；不过，你也可以为某台计算机上的所有网站设置内容过期。

你还可以配置 Web 服务器的内容分级功能，将说明性标签嵌入到网页的 HTTP 头中。某些 Web 浏览器（如 IE 3.0 或更高版本）可以检测这些内容标签，并帮助用户识别可能使人反感的 Web 内容。Web 服务器默认的基于 Internet 内容选择（PICS）的分级系统平台使用由 Internet 内容分级协会（ICRA）开发的系统，该协会根据暴力、裸露、色情及侵犯性语言的级别来对内容进行分级。在设置 Web 内容分级之前，你应该填写 ICRA 问卷以获得为你的特定 Web 内容建议的内容分级。

如果你的网站对公众开放，采取内容分级是个好办法。这样做不会自动让用户滤掉你的网站，因为用户也必须启用内容分级，并在他们的客户端计算机上设置内容权限，这样分级

信息才会影响他们的浏览体验。

设置网站内容的过期时间的步骤如下所述。

(1) 在 IIS 管理器中，展开本地计算机。在要设置内容过期的网站、虚拟目录或文件上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“HTTP 头”选项卡，如图 2-89 是选择“网站”文件夹（可作用于当前 IIS 管理中的所有网站）时的对应选项卡。

(2) 选择“启用内容过期”复选项，下面的许多有关选项将同时激活。对于对时间敏感的材料（例如特定的报价或事件公告），则选中“启用内容过期”复选项，以包括过期信息。浏览器将当前日期与过期日期相比较以决定是显示一个缓存页，还是从服务器请求一个更新的界面。如果选择“立即过期”单选项，则内容将立即过期。该设置强制浏览器总是从服务器上检索有关后续请求的最新内容；如果选择的是“此时间段后过期”单选项，则可设置特定的时间段，超过该时间段后则强制浏览器重新从服务器上检索有关后续请求的内容。如果选择的是“过期时间”单选项，则可以设置特定的日期和时间，超过该日期和时间后则强制浏览器重新从服务器上检索有关后续请求的内容。

“自定义 HTTP 头”列表可将自定义 HTTP 头从 Web 服务器发送到客户端浏览器。自定义头可用来将当前 HTTP 规范中尚不支持的指令从 Web 服务器发送到客户端，例如产品发布时 IIS 尚不支持的更新的 HTTP 头。例如，可以使用自定义 HTTP 头来允许客户端浏览器缓存界面而禁止代理服务器缓存界面。



图 2-89 网站属性对话框“HTTP 头”选项卡

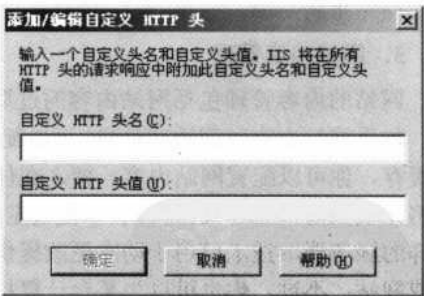


图 2-90 “添加/编辑自定义 HTTP 头”对话框

单击【添加】按钮，打开如图 2-90 所示的对话框。在“自定义 HTTP 头名”和“自定义 HTTP 头值”两文本框中分别键入自定义 HTTP 头的名称和值。自定义头将以 Name:Value 的形式出现在如图 2-89 所示的“自定义 HTTP 头”列表框中。

(3) 单击【应用】按钮，单击【确定】按钮完成配置。

设置内容分级的步骤表述如下。

(1) 在 IIS 管理器中，展开本地计算机。在要设置内容过期的网站、虚拟目录或文件上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“HTTP 头”选项卡，如图 2-82 所示是选择“网站”文件夹（可作用于当前 IIS 管理中的所有网站）时对应的选项卡。

(2) 在“内容分级”栏中单击【编辑分级】按钮，打开如图 2-91 所示的对话框。

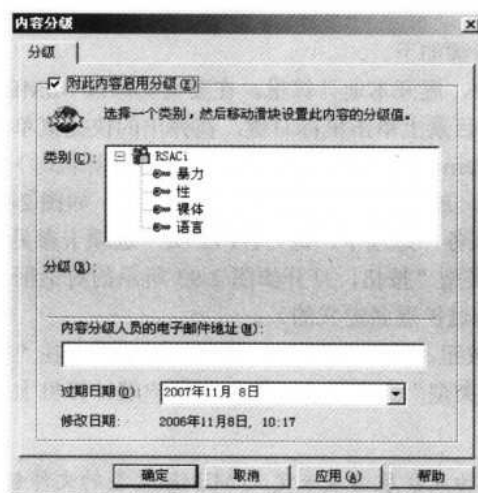


图 2-91 “内容分级”对话框“分级”选项卡

(3) 在“分级”选项卡中选择“对此内容启用分级”复选项。然后在“类别”列表框中选择某个分级类别。拖动或单击分级滑块为该类别设置可能使人反感的资料的级别。每项设置都显示有所分等级的说明。

在“内容分级人员的电子邮件地址”文本框中输入进行内容分级的人的电子邮件地址。在“过期时间”下拉列表框中选择分级截止日期。

(4) 单击【应用】按钮，单击【确定】按钮完成配置。

4. MIME 类型支持管理

Multipurpose Internet Mail Exchange (MIME) 类型说明了 Web 浏览器或邮件应用程序如何处理从服务器接收的文件。例如，当 Web 浏览器请求服务器上的某一项目时，也会请求此对象的 MIME 类型。某些 MIME 类型（例如图形）可以在浏览器内部显示。其他的 MIME 类型（例如文字处理文档）则需要使用外部帮助应用程序来显示。

当 IIS 传递邮件消息给邮件应用程序或传递网页给客户端 Web 浏览器时，IIS 也发送了所传递数据的 MIME 类型。如果存在以特定格式传递的附加或嵌入文件，那么 IIS 就会通知客户端应用程序嵌入或附加文件的 MIME 类型。然后客户端应用程序就知道了如何处理或显示正从 IIS 接收的数据。

IIS 只为具有已在 MIME 类型列表中注册的扩展名的文件提供服务，并且也允许配置其他的 MIME 类型和更改或删除 MIME 类型。

IIS 预配置为识别全局 MIME 类型的默认设置，你在 IIS 中创建的所有网站可以识别这些 MIME 类型。MIME 类型还可以独立于其他的或全局定义的类型，在网站和目录级别上定义。

当在网站或目录级别上查看 MIME 类型时，只显示唯一对应于此级别的类型，并非从上一级别继承的所有类型。如果在较低级别修改 MIME 类型后，又在全局级别上应用相同的 MIME 类型，那么全局级别的 MIME 类型将覆盖在较低级别修改过的 MIME 类型。

如果客户端请求引用了其扩展名未在 MIME 类型中定义的文件扩展名，那么 IIS 将返回一个 404.3 错误。通过添加通配符 (*) MIME 类型，也可以将 IIS 配置成向所有的文件提供服务，而忽略文件扩展名。

设置 MIME 类型的步骤如下。

(1) 在 IIS 管理器中，展开本地计算机。在要向其添加 MIME 类型的计算机、“网站”文件夹、具体网站或网站目录上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“Internet 信息服务”选项卡（选择计算机时），或者“HTTP 头”选项卡（选择“网站”文件夹，或者具体网站、网站目录时），如图 2-92 所示是在 IIS 管理器计算机上的“Internet 信息服务”选项卡，而“HTTP 头”选项卡参见图 2-89。

(2) 单击“MIME 类型”按钮，打开如图 2-93 所示的对话框。在这里列出了系统默认支持 MIME 文件类型（通过扩展名定义的）。

(3) 单击【新建】按钮，打开如图 2-94 所示的对话框。在“扩展名”文本框中，键入文件扩展名；在“MIME 类型”文本框中，键入与客户端计算机上所定义的文件类型完全匹配的说明。



还可以为无扩展名或未定义 MIME 类型的文件创建 MIME 类型。要完成此操作，在“扩展名”文本框中键入星号 (*)，并且在“MIME 类型”文本框中键入 application/octet-stream。

(4) 单击【确定】按钮返回到如图 2-92 所示的对话框。再单击【确定】按钮完成新 MIME 类型的添加。

要删除已添加的 MIME 类型，只需在如图 2-93 所示的对话框列表中选择相应的选项，然后单击【删除】按钮即可。

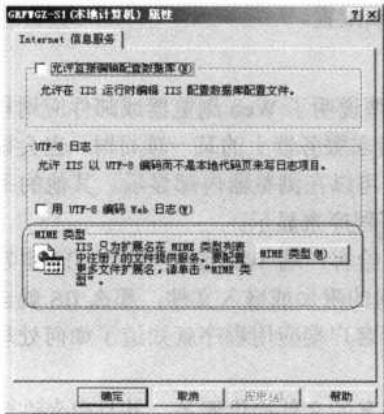


图 2-92 IIS 管理器计算机属性对话框
“Internet 信息服务”选项卡



图 2-93 “MIME 类型”对话框

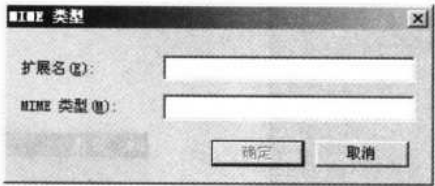


图 2-94 “MIME 类型”对话框

5. 配置允许或拒绝访问的 IP 地址或域名

可以配置网站以允许或拒绝特定计算机、计算机组或域访问网站、目录或文件。例如，如果 Intranet 服务器已连接到 Internet，你可以防止 Internet 用户访问 Web 服务器，方法是仅授予 Intranet 成员访问权限而明确拒绝外部用户的访问。

授予或拒绝对计算机的访问的配置步骤如下。

(1) 在 IIS 管理器中，展开本地计算机。在某个网站、目录或文件上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“目录安全性”（参见图 2-46）或“文件安全性”（参见图 2-68）选项卡。

(2) 在“IP 地址和域名限制”栏中单击【编辑】按钮，打开如图 2-95 所示的对话框。

选择“授权访问”或“拒绝访问”单选项。当选择“拒绝访问”单选项时，将拒绝所有计算机和域的访问权限，但你特别授予访问权限的计算机和域除外；当选择“授权访问”单选项时，将向所有计算机和域授予访问权限，但特别拒绝访问权限的计算机和域除外。

(3) 如果选择了“拒绝访问”单选项，单击【添加】按钮，打开如图 2-96 所示的对话框；如果选择了“授权访问”单选项，单击【添加】按钮，打开如图 2-97 所示的对话框。两个对话框的配置选项是一样的。

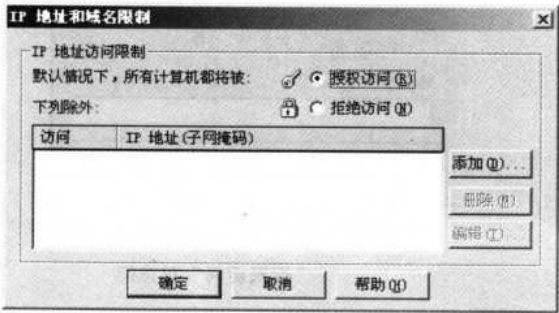


图 2-95 “IP 地址或域名限制”对话框

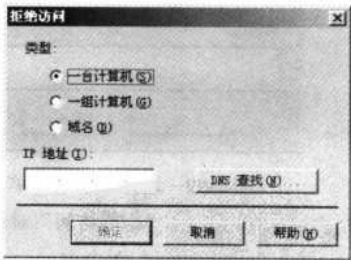


图 2-96 选择“一台计算机”单选项时的“拒绝访问”对话框

(4) 在如图 2-96 或图 2-97 所示的对话框中选择“一台计算机”单选项。单击【DNS 查找】按钮，打开如图 2-98 所示的对话框。在“输入 DNS 名称”文本框中输入要添加的计算机 DNS 名称，然后单击【确定】按钮，按名称而不是按 IP 地址来搜索计算机或域。如果找到，则在“IP 地址”文本框中自动输入它的 IP 地址。

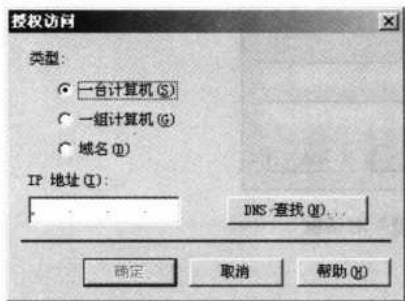


图 2-97 选择“一台计算机”单选项时的“授权访问”对话框



图 2-98 “DNS 查找”对话框

在使用“DNS 查找”功能时，一定要牢记以下信息。

- 它在查找 DNS 地址时导致服务器性能下降。
- 通过代理服务器访问 Web 服务器的用户将使用代理服务器的 IP 地址。
- 通过输入“*.domainname.com”语法，而不是“domainname.com”语法，可纠正某些用户服务器访问问题。

(5) 依次单击【确定】按钮 3 次完成配置。

授予或拒绝对域的访问的配置步骤与上面介绍的“授予或拒绝对计算机的访问”的配置方法基本一样，只是要在如图 2-96 或 2-97 所示的对话框中选择“域名”单选项，此时的两个对话框对应变成如图 2-99 和图 2-100 所示。

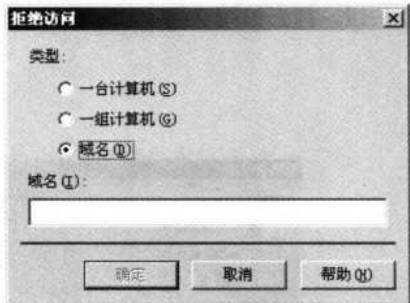


图 2-99 选择“域名”单选项时的“拒绝访问”对话框

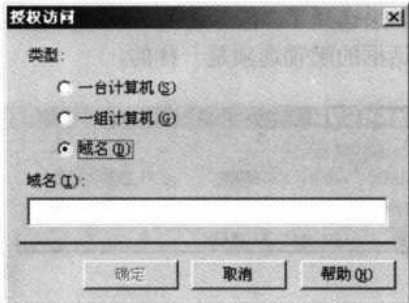


图 2-100 选择“域名”单选项时的“授权访问”对话框

然后在“域名”文本框中键入域名。依次单击【确定】按钮 3 次完成配置。

使用网络标识和子网掩码，可以拒绝或授予一组计算机的访问权限。网络标识是主机的 IP 地址，该计算机通常是“子网”的路由器。子网掩码决定 IP 地址的哪一部分是子网标识而哪一部分是主机标识。子网中的所有计算机具有相同的子网标识和自己特有的主机标识。通过指定网络标识和子网掩码，可以选择一组计算机。

例如，如果主机拥有 IP 地址 172.16.16.1 和子网掩码 255.255.0.0，那么子网中的所有计算机将拥有以 172.16 开头的 IP 地址。要选择子网中的所有计算机，可在“网络标识”文本框中输入 172.16.16.1，在“子网掩码”文本框中输入 255.255.0.0。如果没有划分子网，而且要限制，或者授权访问的一组计算机是整个网段，则可直接输入网络类型，采用默认的子网

掩码。如在“网络标识”文本框中输入 192.168.1.0，在“子网掩码”文本框中输入 255.255.255.0，则表示要拒绝或授权整个 192.168.1.0 网络的计算机。

授予或拒绝对一组计算机的访问的方法与前面介绍的“授予或拒绝对计算机的访问”的配置方法也基本一样，只是要在如图 2-96 或图 2-97 所示的对话框中选择“一组计算机”单选项，此时的两个对话框对应变成如图 2-101 和图 2-102 所示。

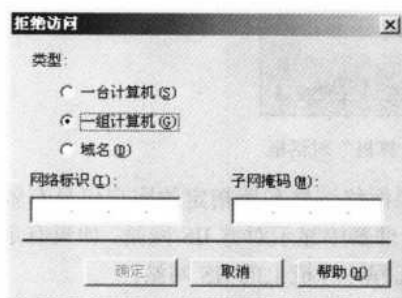


图 2-101 选择“一组计算机”单选项时的“拒绝访问”对话框

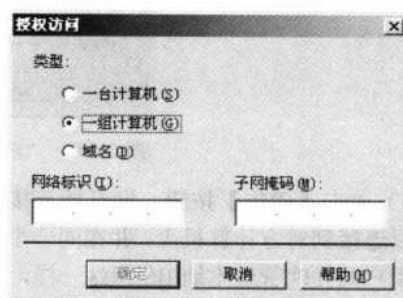


图 2-102 选择“一组计算机”单选项时的“授权访问”对话框

在“网络标识”文本框中键入主机的 IP 地址；在“子网掩码”文本框中键入要授予或拒绝访问的计算机的子网标识（主要是通过子网标识来确定 IP 地址的范围）。最后依次单击【确定】按钮 3 次完成配置。

2.7.5 网站的远程管理

作为网站的管理员，难免会因为某些事而不能时时守候在网站服务器旁边，而此时如果想要对网站服务器进行维护和管理的话，就得使用各种远程管理工具了。网站的远程管理工具主要包括以下 3 种。

- IIS 管理器：你可以在服务器上使用 IIS 管理器来远程连接和管理运行 IIS 4.0、IIS 6.0 或 IIS 5.1（不支持 IIS 3.0）的 Intranet 服务器。
- 终端服务：终端服务不要求你在远程客户端上安装 IIS 管理器，因为一旦连接到运行 IIS 的服务器上，就可以像登录到本地一样使用 IIS 管理器。
- 远程管理（HTML）工具：你可以使用远程管理（HTML）工具从 Intranet 上的任何 Web 浏览器管理 IIS Web 服务器。不过，该版本的远程管理工具只能在运行 IIS 6.0 的服务器上使用。

因为终端服务所涉及到的内容比较多，所以在此不介绍终端服务方案，只在介绍 IIS 管理器和远程管理（HTML）工具方案时进行介绍。

1. 使用 IIS 管理器远程管理 Intranet 服务器

使用 IIS 管理器远程管理 Intranet Web 服务器的具体步骤如下。

- （1）在网络上运行 Windows Server 2003 家族成员的任何计算机上启动 IIS 管理器。
- （2）要连接到远程 IIS 计算机，在 IIS 管理器控制台本地计算机上单击鼠标右键，在弹出的快捷菜单中选择【连接】命令，打开如图 2-103 所示的对话框。在“计算机名”文本框

120 网管员必读——网络应用（第2版）

中键入或浏览要连接到的计算机名，如果对方不允许以匿名方式进行远程连接，则要选择“连接为”复选项，然后在下面输入自己的账户信息。这个账户信息一定要在对方计算机上有效，而且有足够的网站管理权限。

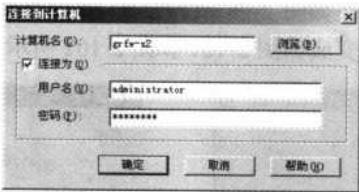


图 2-103 “连接到计算机”对话框

(3) 单击【确定】按钮，即开始连接，如果网络连接和所指定的账户信息有效，则很快就可以连接到对方计算机上，并在同一个 IIS 管理器中显示对方 IIS 网站。如果有足够权限的话，用户同样就管理本地 IIS 网站一样，管理远程计算机上的 IIS 网站。



注意 如果未安装 TCP/IP 和名称解析服务器（如 WINS），则可能无法使用计算机名连接到 IIS 计算机。此时，还可以使用 IIS 计算机的 IP 地址进行连接。

2. 通过控制面板启用远程管理（HTML）工具

要通过“远程管理（HTML）”工具来远程管理 IIS 网站，首先得在“添加或删除程序”中安装所需的组件。组件的位置如图 2-104 所示。



图 2-104 “远程管理（HTML）”工具组件位置

安装后即可通过网络的方式远程管理 Web 网站和其他所有在 IIS 管理器中部署的站点，如网站、FTP 站点和邮件服务器等。具体步骤如下。

(1) 在远程计算机 IE 浏览器地址栏中键入 https://hostname:8098（注意，此处必须为安全连接“https”，而非普通的“http”），其中 hostname 是要连接和管理的计算机名称，8098 是远程管理（HTML）所使用的端口。也可使用 https://IPaddress:8098 进行远程连接，其中 IPaddress 为要连接和管理的计算机 IP 地址。如现在要远程管理 grfwg-s1 上的 IIS，则可以在浏览器地址栏中输入 https://grfwg-s1:8098，首先打开的是一个如图 2-105 所示的身份验证窗口，在其中要输入有权限访问远程 IIS 的用户账户信息。这个账户必须是远程计算机所属计算机，或者网络有效的账户。

(2) 单击【确定】按钮，弹出一个警告提示，如图 2-106 所示。提示用户当启用了 IE 浏览器的增加安全配置时，会增强服务器的安全性，但同时也会影响到远程服务器的访问。



图 2-105 远程连接的身份验证窗口



图 2-106 远程连接的警告提示框

(3) 单击【确定】按钮后，打开如图 2-107 所示的远程 IIS 管理界面。在这里显示了可以通过此方法管理 IIS 的设置选项，可设置选项非常多。在如图 2-107 所示的“欢迎使用”界面中就可设置管理员密码、服务器名、默认界面，还可以连接到微软公司的社区（在连接了互联网的情况下）。



图 2-107 IIS 远程管理窗口“欢迎使用”界面

(4) 在中间的工具条中单击【状态】按钮，打开如图 2-108 所示界面。在这里可以查看状态警报、系统资源和系统信息。还可通过“安装新证书”链接项为 IIS 服务器安装新的证书。



图 2-108 IIS 远程管理窗口“状态”界面

122 网管员必读——网络应用（第2版）

(5) 单击工具条中的【站点】按钮，打开如图 2-109 所示界面。从“网站配置”界面中，在这里你可以了解当前 IIS 中创建的网站，并完成创建网站、修改网站设置、删除网站、暂停网站、停止网站、启动网站等任务之一。



图 2-109 IIS 远程管理窗口“站点”界面

注意 通过服务器管理的 Web 界面修改网站时需要注意的一点是，虽然所有可用的网站都在列表中列出，但是你能只能修改最初通过 Web 界面创建的那些站点。你对其他站点进行的修改仅限于将它们暂停、启动和停止。

(6) 单击工具条中的【Web 服务器】按钮，如图 2-110 所示。在打开的界面中可以对 Web 服务器进行全面设置，如 Web 主设置、设置 Web 执行权限、配置 Web 日志设置、FTP 主设置、显示 FTP 消息、配置 FTP 日志设置等。从中可以看出，在此既可设置 Web 网站，也可设置 FTP 站点。



图 2-110 IIS 远程管理窗口“Web 服务器”界面

(7) 单击工具条中的【电子邮件】按钮，打开如图 2-111 所示界面。在这里可以查看对邮件服务器进行全面的设置。



图 2-111 IIS 远程管理窗口“电子邮件”界面

(8) 单击工具条中的【网络】按钮，打开如图 2-112 所示界面。在这里可以查看对 Web 服务器进行全面的网络设置，其中包括管理员密码、网络接口、应用服务器上的网络设置、服务器名和所在成员身份等。



图 2-112 IIS 远程管理窗口“网络”界面

(9) 单击工具条中的【用户】按钮，打开如图 2-113 所示界面。在此页中，你可以创建、编辑和删除服务器上的本地用户和组。还可以更改每一个组的成员。如果服务器是一个域的成员，则不必在该服务器上创建任何用户。此界面的主要用途是向本地组添加一个或多个域成员。你可以使用域用户和组账户来控制对服务器上的资源的访问。还可以使用域管理工具来对域用户和域组进行管理。



图 2-113 IIS 远程管理窗口“用户”界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

124 网管员必读——网络应用（第2版）

（10）单击工具条中的【维护】按钮，打开如图 2-114 所示界面。在这里可以对 Web 服务器进行基本的维护，如服务器上的日期和时间设置、服务器日志记录的设置、服务器的警报电子邮件设置、连接到 Web 服务器桌面等。



图 2-114 IIS 远程管理窗口“维护”界面

（11）如果对远程管理 Web 服务器不是很熟悉，在这里还需要非常全面的教程，可以通过单击界面中的【帮助】按钮，打开帮助窗口，打开如图 2-115 所示帮助界面。在这里对如何维护 Web 服务器进行了详细的介绍。即使是生手，也完全可以从中学习到专业的 Web 服务器维护知识。



图 2-115 IIS 远程管理窗口“帮助”界面

因为篇幅关系，有关命令方式的网站管理方法就不再介绍了，关于动态域名解析和端口映射方面的配置方法在本书的第 1 章已有具体介绍，参见即可。下章将介绍另一种主要的网站建设方案——Apache Server 方案。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

CHAPTER

3

第 3 章 Apache 2.2 Web 网站配置

在上一章我们介绍了利用 Windows Server 2003 R2 系统自带的 IIS 6.0 建设 Web 网站的方法，本章要介绍另一种当前最著名的网站建设方案——Apache HTTP Server 方案。不过，在本书中，将介绍 Apache HTTP Server 的最新 2.2.3 版本的方案，而不是在第一版《网管员必读——网络应用》中介绍的 2.0.47 核心版本。

Apache 的 Web 服务器方案是全球用户应用最广的方案，占到了整个 Web 服务器方案的 60% 以上，是微软公司的 IIS 方案的市场占有率的两倍以上。相对 IIS 方案来说，功能更加强大，性能和安全性也更好，但因为是采用配置文件方式进行配置的，所以对于大多数用户来说，配置起来会感觉有些不方便。其实只要理解了配置文件的结构和各指令的用途及使用方法，Apache 配置文件的配置也是很简单的，加上它的功能非常强大，IIS 有的它都有，IIS 没有的，它也有许多。另外，由于它采用的是纯文本配置文件配置方式，所以整体性能和安全性会明显高于图形界面的 IIS 方案。不过，由于本书的篇幅限制原因，在本章不可能对 Apache 方案的各个方面进行详细介绍，仅介绍基本的全局配置方法。本章有关 Apache 模块和指令部分参考或者摘选了金步国先生为 Apache 程序所翻译的帮助文档，在此深表感谢！

本章重点

- Apache 服务器的基本结构
- Apache 服务器配置文件基本组成
- Apache 服务器的安装调试
- Apache 服务器的主要模块功能
- Apache 服务器核心模块指令及各自的主要功能和语法
- Apache 服务器的全局配置

3.1 Apache 2.2 基础

Apache 的最早版本是 1995 年 12 月 1 日发布的，最初的 Apache 版本由美国伊利诺斯大学香槟分校（University of Illinois, Urbana-Champaign）国家超级计算应用中心（NCSA）的 Rob McCool 先生开发的 the Public Domain HTTPS Daemon 程序发展而来。

Apache 具有强大的功能，如基于名字和 IP 地址的虚拟主机、用户验证、URL 重定向（URL Rewrite）、SSI（服务器端嵌入）、SSL（安全套接层）等功能特性。Apache 目前的最新版本为 2.2.3，安装的 MSI 包程序为 4.3MB。可以到它的主页：<http://www.apache.org> 上下载，也可在其他网站下载，如华军软件园、天空软件站等。互联网上大概有 65% 的 Web 服务器使用 Apache HTTP 服务器，这个数字是通过 Netcraft 网站了解的。如果你对互联网上 Web 服务器的调查报告感兴趣的话，可以访问：http://news.netcraft.com/archives/web_server_survey.html。图 3-1 是自 1995 年至 2006 年 12 月的调查结果。从中可以看出，全球使用 Apache 作为 Web 服务器的占到了 60% 以上，而使用微软 IIS 的基本上在 20% 左右，其他的就更低了。

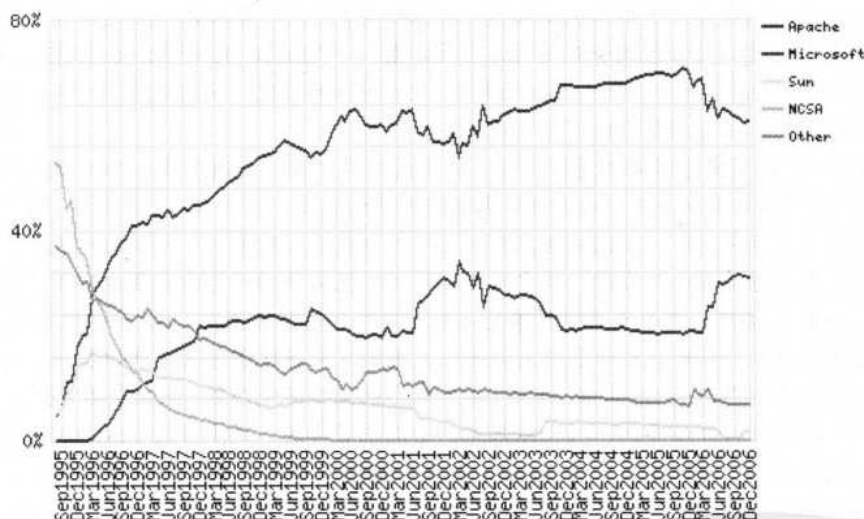


图 3-1 全球互联网上使用 Apache 作为 Web 服务器的用户比例

Apache 在网站服务器方面的应用主要是在 UNIX 和 Linux 系统下，在 Windows 系统平台下，功能相对较弱。但为了照顾大多数 Windows 用户，本节仍以 Windows 平台下的应用为例进行介绍，顺便介绍一些在 UNIX 和 Linux 下特有的功能。另外，因为许多网友对 Apache 这个高性能 Web 服务器软件仍比较陌生，所以在正式介绍利用 Apache 程序架设 Web 虚拟服务器之前，非常有必要对 Apache 程序的基本组成和使用方法进行了了解。

3.1.1 Apache 2.2 程序的组成

在 2.2 以前的版本中，Apache 服务器程序使用了 3 个配置文件：`httpd.conf`、`access.conf`

和 `srm.conf`，来配置 Apache 服务器的行为。`httpd.conf` 提供了最基本的服务器配置，是对守护程序 `httpd` 如何运行的技术描述；`srm.conf` 是服务器的资源映射文件，告诉服务器各种文件的 MIME 类型，以及如何支持这些文件；`access.conf` 用于配置服务器的访问权限，控制不同用户和计算机的访问限制；这 3 个配置文件控制着服务器各个方面的特性，因此为了正常运行服务器便需要设置好这 3 个文件。

除了这 3 个设置文件之外，Apache 还使用 `mime.types` 文件用于标识不同文件对应的 MIME 类型，`magic` 文件可以设置不同 MIME 类型文件的一些特殊标识，使得 Apache 服务器从文档后缀不能判断出文件的 MIME 类型时，能通过文件内容中的这些特殊标记来判断文档的 MIME 类型。

而在 2.2 版本中，Apache 将原来 `httpd.conf`、`srm.conf` 与 `access.conf` 中的所有配置参数均放在一个配置文件 `httpd.conf` 中，所以现在只需要配置这一文件就可以全面配置 Apache 服务器了。这个文件在程序安装路径下的 `conf` 目录下，如图 3-2 所示。对于这个配置文件，可以不加改动运行 Apache 服务器。但如果需要调整 Apache 服务器的性能，以及增加对某种特性的支持，就需要了解这些设置参数的含义。



图 3-2 程序安装路径下的 `conf` 目录下的 `httpd.conf` 文件

关于 Apache 服务器的性能，在 Internet 上存在很大的争议，基本上使用 Apache 的使用者都不怀疑它的优秀性能，Apache 也支撑很多著名的高负载的网站，但是在商业机构的评测中，Apache 往往得分不高。究其原因是极少用户能对 Apache 服务器进行最佳的性能配置，多数是采取了默认配置。而 Apache 服务器本身的默认配置绝不是最优化和最高效的，而是要适应几乎所有种类操作系统、所有种类硬件下的设置，多平台的软件不可能为特定平台和特定硬件提供最优化的默认配置。因此要使用 Apache 的时候，性能调整是必不可少的。

以下列出了 Apache HTTP 服务器中所有的可执行程序：

- `Httpd`：Apache HTTP 服务器。
- `Apachectl`：Apache HTTP 服务器控制接口，用于配置文件测试。
- `Ab`：Apache HTTP 服务器性能测试工具。
- `Apxs`：Apache 功能扩展工具。
- `Configure`：配置源代码树。

128 网管员必读——网络应用（第2版）

- Dbmmanage: 建立和更新 DBM 形式（一种饮食用户名和密码等信息，便于进行数据库管理的二进制数据文件，类似于 txt 文本）的基本认证文件。
- Htcacheclean: 清理磁盘缓冲区。
- Htdigest: 建立和更新摘要认证文件。
- Htdbm: 操作 DBM 数据库文件。
- Htpasswd: 建立和更新基本认证文件。
- httxt2dbm: 创建 RewriteMap 指令需要使用的 DBM 文件。
- logresolve: 将 Apache 日志文件中的 IP 地址解析为主机名。
- rotatelog: 滚动 Apache 日志而无须终止服务器。
- suexec: 为 Exec 切换用户。

3.1.2 Apache 2.2 的新特性

我们在第一版的《网管员必读——网络应用》中介绍了 Apache 2.0 的应用，本章要采用最新的核心——Apache 2.2 进行介绍。在此先来了解这一版本相对 Apache 2.0 来讲有哪些新的特性。

1. 核心程序的功能增强

在程序核心方面，主要改进体现在以下几个功能方面的增强。

- 认证/授权 (Authn/Authz) 在 2.0 版本中捆绑在一起的认证 (authentication) 与授权 (authorization) 模块现在被分开了。新的 mod_authn_alias 模块可以极大地简化某些身份认证的配置。具体请参见本节后面将要介绍的“模块增强”和“程序增强和针对开发者的改进”部分的内容，以了解更多有关这些变更对于模块使用者和模块开发者的影响。
- 缓冲 mod_cache、mod_disk_cache、mod_mem_cache 三全模块经历了诸多修改以后现在已经具备了合格的产品质量了。新增加的 htcacheclean 工具可以用来清理 mod_disk_cache 模块使用的缓冲存储区。
- 配置 默认的配置布局已经被简化并模块化了。启用常用特性的配置片段现在已经和 Apache 捆绑在一起，可以被轻易地添加到主配置文件中。
- 优雅停止 (graceful-stop) prefork、worker、event 多路处理模块 (MPM) 现在允许 httpd 通过 graceful-stop 信号被优雅地停止。用户还可以用新增的 GracefulShutdownTimeout 指令指定一个超时时间，在超过指定的时间以后 httpd 将会强行终止，而无论请求所处的服务状态如何。
- 代理 新增的 mod_proxy_balancer 模块为 mod_proxy 模块提供了负载均衡服务。新增的 mod_proxy_ajp 模块为 Apache Tomcat 程序使用的 Apache JServ Protocol version 1.3 提供了支持。
- 正则表达式库更新 5.0 版的 Perl 兼容正则表达式库 (PCRE) 已经被包含进来了。httpd 现在可以通过使用 “with-pcre” 参数选项编译使用系统中已经安装好的 PCRE。

- 智能过滤器 `mod_filter` 可以进行输出过滤器链的动态配置。它允许过滤器按照请求头、应答头或环境变量有条件地插入，这样就避免了许多在 Apache 2.0 体系结构中存在的过滤器之间的依赖性和顺序问题。
- 大文件支持 `httpd` 现在已经被构建为在现代的 32 位 UNIX 系统上支持大于 2GB 的文件。而且也可以处理大于 2GB 的请求体（request body）。
- Event MPM Event 多路处理模块（MPM）使用一个单独隔开的线程处理持久连接（Keep Alive），而以前的版本中，HTTP 持久连接要求 `httpd` 专门拿出一个工作者（Worker，也就是一个进程/线程）来处理它。这个专用的工作者在持久连接超时前不能被重新使用。
- SQL 数据库支持 `mod_dbd` 模块和 `apr_dbd` 框架（framework）一起为需要使用数据库的模块提供直接的支持。在线程化的 MPM 中还能支持连接缓冲池。但是，这个特性尚未包含在标准的 Windows 版 Apache 中。

2. 模块增强

Apache 的一个重要特点就是功能模块化，在新版本中，功能模块也有所增强，具体表现如下。

- 认证/授权（Authn/Authz） `aaa` 目录下的模块已经被重新命名，并统一放在 `modules` 目录下，提供了对摘要认证（digest authentication）的更好支持。例如，以前版本的 `mod_auth`，现已经被分割成 `mod_auth_basic` 和 `mod_authn_file` 两个模块；以前版本的 `mod_auth_dbm` 现在更名为 `mod_authn_dbm`；以前版本的 `mod_access` 现在更名为 `mod_authz_host`。还新增了一个 `mod_authn_alias` 模块用于简化某些认证配置。有关各模块的简要功能说明将在本章后面的列表中介绍。
- `mod_authnz_ldap` 这个模块是 2.0 版 `mod_auth_ldap` 模块到 2.2 版的 Authn/Authz 框架的一个移植。新的特性包括使用 LDAP 属性值和 `Require` 指令中复杂的搜索过滤器。
- `mod_info` 添加了一个新的“`?config`”参数，可以用来显示被 Apache 分析过的配置指令，包括它们的文件名和行号。该模块还显示所有请求钩子（request hook）的顺序和额外的编译信息，有些类似于 `httpd -V`。
- `mod_ssl` 添加了 RFC 2817 支持，它允许连接从明文提升到 TLS 加密。
- `mod_imagemap` `mod_imap` 模块已经被重命名为 `mod_imagemap`，以避免用户产生混淆和疑惑。

3. 程序增强和针对开发者的改进

除了以上基本功能的增强外，Apache 程序本身也进行了许多改进和增强，具体表现如下。

- `httpd` 进程增强 添加了一个新的命令行选项“`-M`”用来列出基于当前配置加载的所有模块。不同于“`-l`”选项的是，它还列出了通过 `mod_so` 加载的 DSO（动态共享对象）。
- 新增 `httxt2dbm` 这是一个用于从文本输入产生 `dbm` 文件（一种数据库文件）的程序，目的是为了能够在 `RewriteMap` 中使用 `dbm` 映射表（map）类型。

130 网管员必读——网络应用（第2版）

- APR 1.0 API Apache 2.2 使用 APR 1.0 API，但所有反对使用的函数和符号已经从 APR 和 APR-Util 中清除掉了。
- 认证/授权（Authn/Authz） 原来捆绑在一起的认证和授权模块已经被按照下列规则进行了重命名。
 - ✧ mod_auth_*：实现 HTTP 认证机制的模块。
 - ✧ mod_authn_*：实现后端认证支持者的模块。
 - ✧ mod_authz_*：实现授权（或访问）的模块。
 - ✧ mod_authnz_*：同时实现认证和授权的模块。
- 连接错误日志 添加了一个新的 ap_log_cerror 函数，用于记录客户端连接时发生的错误，并且在记录时包含客户端 IP 地址。
- 添加了一个测试配置的钩子（hook） 添加了一个新的 test_config 钩子，可以在用户向 httpd 传递“-t”选项时执行包含特定代码的模块。
- 设置线程型 MPM 所使用的栈空间大小 新增的 ThreadStackSize 指令可以用来限制所有线程型 MPM（多路处理模块）所使用的栈大小。一些默认栈空间较小的平台上的第三方模块需要使用它指定栈空间的大小。
- 输出过滤器协议处理 在以前的版本中，每个过滤器都要确保自身能够产生正确的应答头。现在过滤器可以调用 ap_register_output_filter_protocol 或 ap_filter_protocol 指令来委托 mod_filter 模块进行协议管理。
- 添加了监视钩子（Monitor hook） 监视钩子可以让模块运行父进程中事先安排好的工作。
- 正则表达式 API 的变化 pcreposix.h 头文件现在被 ap_regex.h 头文件取代了。原来老的 POSIX.2 regex.h 实现现在位于 ap_命名空间下（由 ap_regex.h 提供）。比如，原来的 regcomp, regexexec 调用现在要修改成 ap_regcomp, ap_regcomp 调用。
- 新增 DBD 框架（SQL 数据库 API） 在 1.x 和 2.0 版本中，需要 SQL 支持的模块必须自己管理数据库。为了不重新发明轮子，Apache 2.1 及以后的版本提供了 ap_dbd API 来管理数据库连接（包括对线程型和非线程型 MPM 进行优化），同时 APR 1.2 及以后版本也提供了 apr_dbd API 与数据库打交道。

新模块应当使用这些 API 来进行数据库操作，现存的应用程序应当进行透明的升级或使用推荐选项来使用这些 API。

3.2 Apache 服务器配置文件

本节要介绍的是 Apache 服务器的配置文件 http.conf 的基础知识，包括配置文件的基本组成、配置段、模块、指令等。这在使用配置时非常重要，毕竟它不像 Windows 系统平台那样直观。

3.2.1 Apache 配置文件基础

在 mod_mime 模块中，可使用的指令包括<IfDefine>、Include 和 TypesConfig。Apache

的配置文件是包含若干指令的纯文本文件。主配置文件通常叫 `httpd.conf`，其位置是编译时确定的，但可以用命令行参数 `-f` 来改变。另外，还可以用 `Include` 指令和通配符附加许多其他配置文件。任何配置文件都可以使用任何指令。只有在启动或重新启动 Apache 后，主配置文件的更改才会生效。

除此之外，服务器还会读取一个包含 MIME 文件类型的文件，其文件名由 `TypesConfig` 指令确定，默认值是 `mime.types`。

1. 配置文件的语法

Apache 配置文件的每一行包含一个指令，在行尾使用反斜杠（`\`）可以表示续行，但是反斜杠与下一行之间不能有任何其他字符（包括空白字符）。

配置文件中的指令是不区分大小写的，但是指令的参数（`argument`）通常是大小写敏感的。以“`#`”符号开头的行被视为注解并被忽略，如果想让相应行生效，则可以去掉相应行的“`#`”符号。注解不能出现在指令的后边，这一点与我们平时的使用习惯不一样，一定要注意。空白行和指令前的空白字符将被忽略。

在 UNIX 和 Linux 系统下，可以用 `apachectl configtest` 命令检查配置文件中的错误，而无须启动 Apache 服务器。

2. 模块

Apache 是模块化的服务器，这意味着核心中只包含实现最基本功能的模块。模块是 Apache 的重要组成部分，是 Apache 核心功能的扩展，也是 Apache 具有如此强大功能的基础，而且模块还在不断扩展。Apache 的扩展功能就是通过以模块的方式来动态加载。加载时所用的指令有两个：`<IfModule>` 和 `LoadModule`。

Apache 对独立模块 DSO 的支持是建立在只能被静态编译进 Apache 核心的 `mod_so` 基础之上的，这是除 `core` 以外唯一不能作为 DSO 存在的模块，而其他所有已发布的 Apache 模块，都可以通过安装文档中阐述的编译选项——`enable-module=shared` 被独立地编译成 DSO 并使之生效。一个被编译为 `mod_foo.so` 的 DSO 模块，可以在 `httpd.conf` 中使用 `mod_so` 的 `LoadModule` 指令，在服务器启动或重新启动时被加载。

如果服务器在编译时包含了 DSO（动态共享对象）模块，那么各模块可以独立编译，并可随时用 `LoadModule` 指令加载；否则，要增加或删除模块必须重新编译整个 Apache。用于特定模块的指令可以用 `<IfModule>` 指令包含起来，使之有条件地生效。用命令行参数“`-l`”可以查看已经编译到服务器中的模块。

模块可以在编译时被静态包含到 `httpd` 二进制文件中，也可以编译成独立于 `httpd` 二进制文件的 DSO。在默认情况下，只有 `base` 组的模块被编译进了服务器，如图 3-3 所示的是在 `httpd.conf` 配置文件中默认采用 `LoadModule` 加载的模块（前面没有注释符“`#`”的部分）。

DSO 模块可以与服务器一起编译，也可以用 Apache 扩展工具（`apxs`）单独编译。新提供的支持程序 `apxs`（APache eXtenSion）可以在 Apache 源代码树之外编译基于 DSO 的模块，从而简化了 Apache DSO 模块的建立过程。其原理很简单：安装 Apache 时，`configure` 的 `make install` 命令会安装 Apache C 头文件，并把依赖于特定平台的编译器和连接器参数传给 `apxs` 程序，使用户可以脱离 Apache 的发布源代码树编译其模块源代码，而不改变支持 DSO 的编译器和连接器的参数。



图 3-3 在 httpd.conf 配置文件中默认采用 LoadModule 加载的模块

3. 指令的作用域

指令的作用域是指指令的有效区域。主配置文件中的指令对整个服务器都有效。如果只想改变某一部分的配置，可以把指令嵌入到<Directory>、<DirectoryMatch>、<Files>、<FilesMatch>、<Location>和<LocationMatch>配置段中，这样就可以限制指令的作用域为文件系统中的某些位置或特定的 URL。这些配置段还可以进行嵌套，以进行更精细的配置。

Apache 还具备同时支持多个站点的能力，称为虚拟主机。<VirtualHost>配置段中的指令仅对该段中的特定站点（虚拟主机）有效。

虽然大多数指令可以包含在任意的配置段中，但是某些指令仅在某些特定的范围内才有意义。比如，控制进程建立的指令仅在主服务器范围内有效。要查询一个指令被应用于哪些配置段中，可以查看该指令的作用域项。更详细的介绍请参见下节将要介绍的配置段说明。

4. .htaccess 文件

Apache 可以使用分布在整个网站文件目录树结构中的特殊文件来进行分散配置，这些特殊的文件通常叫.htaccess，但是也可以用 AccessFileName 指令来改变它的名字。htaccess 文件中指令的作用域是存放它的那个目录及其所有子目录。htaccess 文件的语法与主配置文件相同。由于对每次请求都会读取.htaccess 文件，所以对这些文件的修改会立即生效。

要了解一个指令是否可以用在.htaccess 文件中，可以查阅该指令的作用域项。服务器管理员可以在主配置文件中使 AllowOverride 指令来决定哪些指令可以在.htaccess 文件中生效。

3.2.2 配置段和容器

“配置段”和“容器”都是用来指定配置文件的作用范围的。配置文件中指令的作用范围可能是整个服务器，也可能是特定的目录、文件、主机、URL。本节将要介绍的是如何使用配置段及.htaccess 文件来改变配置指令的作用范围。

1. 配置段和容器的类型

配置段的类型包括在 `core`、`mod_version` 和 `mod_proxy` 3 个模块中，可以使用的指令包括：`<Directory>`、`<DirectoryMatch>`、`<Files>`、`<FilesMatch>`、`<IfDefine>`、`<IfModule>`、`<IfVersion>`、`<Location>`、`<LocationMatch>`、`<Proxy>`、`<ProxyMatch>` 和 `<VirtualHost>`。这些指令都是配置段的容器。

容器有两种基本类型。大多数容器是针对各个请求的，包含于其中的指令仅对该容器匹配的请求起作用，而容器 `<IfDefine>`、`<IfModule>`、`<IfVersion>` 仅在启动和重新启动时起作用，如果在启动时指定的条件成立，则其中的指令对所有的请求都有效，否则将被忽略。

`<IfDefine>` 容器中的指令只有在 `httpd` 命令行中设定了特定的参数后才有效。下面的示例中限定只有在服务器用 `httpd -DClosedForNow` 方式启动时，所有的请求才会被重定向到另一个站点：

```
<IfDefine ClosedForNow>
  Redirect / http://otherserver.example.com/
</IfDefine>
```

`<IfModule>` 容器与 `<IfDefine>` 很相似，但是其中的指令只有当服务器启用特定的模块时才有效（或是被静态地编译进了服务器，或是被动态装载进了服务器）。注意，配置文件中该模块的装载指令 `LoadModule` 行必须出现在此容器之前。这个容器应该仅用于无论特定模块是否安装，配置文件都能正常运转的场合；而不应该用于容器中的指令在任何情况下都必须生效的场合，因为它会抑制类似模块没找到之类的有用出错信息。

下面的示例中，指定 `MimeMagicFiles` 指令仅当 `mod_mime_magic` 模块启用时才有效。

```
<IfModule mod_mime_magic.c>
  MimeMagicFile conf/magic
</IfModule>
```

`<IfVersion>` 指令与 `<IfDefine>` 和 `<IfModule>` 也很相似，但是其中的指令只有当正在执行的服务器版本与指定的版本要求相符时才有效。这个模块被设计用于测试套件，以及在一个存在多个不同 `httpd` 版本的大型网络中需要针对不同版本使用不同配置的情况。

```
<IfVersion >= 2.1> # 仅在版本高于 2.1.0 的时候才生效
</IfVersion>
```

`<IfDefine>`、`<IfModule>`、`<IfVersion>` 都可以在条件前加一个“!”符号以实现条件的否定，而且都可以嵌套以实现更复杂的配置。

2. 文件系统和网络空间

最常用的配置段是针对文件系统和网络空间特定位置的配置段。首先必须理解文件系统和网络空间这两个概念的区别：文件系统是指操作系统所看见的磁盘视图，比如，在 UNIX 系统中，Apache 会被默认安装到“`/usr/local/apache2.2`”目录下，在 Windows 系统中，Apache 会被默认安装到“`Program Files/Apache Software Foundation/Apache2.2`”目录下。相反，网络空间是网站被 Web 服务器发送及被客户在浏览器中所看到的视图。在 Windows 平台下，网络空间的默认安装路径为“`Program Files/Apache Software Foundation/Apache2.2/htdocs`”。由于网页可以从数据库或其他地方动态生成，因此，网络空间无须直接映射到文件系统中。



注意

Apache 始终用正斜杠而不是反斜杠作为路径的分隔符,即使是在 Windows 平台中。

1) 文件系统容器

<Directory> 和 <Files> 指令与其相应的正则表达式版本 (<DirectoryMatch> 和 <FilesMatch>) 一起作用于文件系统的特定部分。<Directory> 配置段中的指令作用于指定的文件系统目录及其所有子目录，.htaccess 文件可以达到同样的效果。在下面的示例中，/var/web/dir1 及其所有子目录被允许进行目录索引。

```
<Directory /var/web/dir1>
    Options +Indexes
</Directory>
```

<Files> 配置段中的指令作用于特定的文件名，而无论这个文件实际存在于哪个目录下。下面的示例中的配置指令如果出现在配置文件的主服务器段，则会拒绝对位于任何目录下的 private.html 的访问。

```
<Files private.html>
    Order allow,deny
    Deny from all
</Files>
```

<Files> 和 <Directory> 段的组合可以作用于文件系统上的特定文件。下面的示例中的配置会拒绝对 /var/web/dir1/private.html、/var/web/dir1/subdir2/private.html、/var/web/dir1/subdir3/private.html 等任何 /var/web/dir1/ 目录下的 private.html 的访问。

```
<Directory /var/web/dir1>
    <Files private.html>
        Order allow,deny
        Deny from all
    </Files>
</Directory>
```

2) 网络空间容器

<Location> 指令与其相应的正则表达式版本 (<LocationMatch>) 一起作用于网络空间的特定部分。下面的示例中的配置会拒绝对任何以 “/private” 开头的 URL 路径的访问，如 http://yoursite.example.com/private、http://yoursite.example.com/private123、http://yoursite.example.com/private/dir/file.html 等所有以 “/private” 开头的 URL 路径。

```
<Location /private>
    Order Allow,Deny
    Deny from all
</Location>
```

<Location> 指令与文件系统无关，下面的示例演示了如何将特定的 URL 映射到 Apache 内部的处理器 mod_status 中，而并不要求文件系统中确实存在 server-status 文件。

```
<Location /server-status>
```



```
SetHandler server-status
</Location>
```

3) 通配符和正则表达式

<Directory>、<Files>、<Location>指令可以使用与 C 标准库中的 fnmatch 类似的 shell 风格的通配符。“*”匹配任何字符串，“?”匹配任何单个的字符，“[seq]”匹配 seq 序列中的任何字符，“/”符号不被任何通配符所匹配，所以必须显式地使用。

如果需要更复杂的匹配，这些容器都有一个对应的正则版本：<DirectoryMatch>、<FilesMatch>、<LocationMatch>，可以使用与 Perl 兼容的正则表达式，以提供更复杂的匹配。下面的示例使用非正则表达式的通配符来改变所有用户目录的配置。

```
<Directory /home/*/public_html>
Options Indexes
</Directory>
```

下例是使用正则表达式一次性拒绝对多种图形文件的访问。

```
<FilesMatch \.(?:gif|jpe?g|png)$>
Order allow,deny
Deny from all
</FilesMatch>
```

4) 选择文件系统容器，还是网络空间容器

选择使用文件系统容器，还是使用网络空间容器其实很简单。当指令作用于文件系统时，总是用<Directory>或<Files>；而当指令作用于不存在于文件系统中的对象时，就用<Location>，比如一个由数据库生成的网页。一定不要试图用<Location>去限制对文件系统中的对象的访问，因为许多不同的网络空间路径可能会映射到同一个文件系统目录，从而导致访问限制被突破。比如：

```
<Location /dir/>
Order allow,deny
Deny from all
</Location>
```

上述配置对 http://yoursite.example.com/dir/请求的确起作用。但是，设想在一个不区分大小写的文件系统中，这个访问限制会被 http://yoursite.example.com/DIR/请求轻易突破。而<Directory>指令才会真正作用于对这个位置的任何形式的请求。但是，有一个例外，就是 UNIX 文件系统中的符号连接（软连接），符号连接可以使同一个目录出现在文件系统中的多个位置。<Directory>指令将不重设路径名而直接追踪符号连接，因此，对于安全要求最高的，应该用 Options 指令禁止对符号连接的追踪。

同时，也不要认为使用大小写敏感的文件系统就无所谓了，因为有很多方法可以将不同的网络空间路径映射到同一个文件系统路径中，所以，应当尽可能使用文件系统容器。但是也有一个例外，就是把访问限制放在<Location />配置段中可以很安全地作用于除了某些特定 URL 以外的所有 URL。

3. 虚拟主机

“虚拟主机”是指在一个机器上运行多个网站（比如，www.company1.com 和

136 网管员必读——网络应用（第2版）

www.company2.com)。如果每个网站拥有不同的 IP 地址，则虚拟主机可以是“基于 IP”的；如果只有一个 IP 地址，也可以是“基于主机名”的，其实现对最终用户是透明的。这一点，其实在介绍 IIS 网站架设中也有类似的说明，那就是网站的标识，它既可以基于 IP 地址，也可以基于“主机头值”（也就是域名），还可以基于端口。

Apache 是率先支持基于 IP 的虚拟主机的服务器之一。1.1 及其更新版本同时支持基于 IP 和基于主机名的虚拟主机。虚拟主机中所用的容器就是<VirtualHost>，它作用于特定的虚拟主机，为同一个机器上具有不同配置的多个主机提供支持。

有关虚拟主机的配置方法将在本章后面具体介绍。

4. 代理

<Proxy>和<ProxyMatch>容器中的指令仅作用于通过 mod_proxy 代理服务器访问的、与指定 URL 匹配的站点。下面的示例中的配置会拒绝通过代理服务器访问 cnn.com 站点。

```
<Proxy http://cnn.com/*>  
    Order allow,deny  
    Deny from all  
</Proxy>
```

5. 总结

以上介绍了几种类型的容器及所用的指令，查阅指令的作用域，就可以知道哪些指令可以出现在哪些配置段中。从语法上看，允许在<Directory>段中使用的指令当然也可以在<DirectoryMatch>、<Files>、<FilesMatch>、<Location>、<LocationMatch>、<Proxy>、<ProxyMatch>段中使用，但也有例外：

AllowOverride 指令只能出现在<Directory>段中。

Options（参数选项）中的 FollowSymLinks 和 SymLinksIfOwnerMatch 只能出现在<Directory>段或者.htaccess 文件中。Options 指令不能用于<Files>和<FilesMatch>段。

除了各自的应用范围不同之外，它们之间有些配置段还是可以合并的。配置段会按非常特别的顺序依次生效，由于这会对配置指令的处理结果产生重大影响，因此理解它的流程非常重要。

合并的顺序如下。

（1）<Directory>（除了正则表达式）和.htaccess 同时处理（如果允许的话，.htaccess 的设置会覆盖<Directory>的设置）；

（2）<DirectoryMatch>（和<Directory ~>）；

（3）<Files>和<FilesMatch>同时处理；

（4）<Location>和<LocationMatch>同时处理。

除了<Directory>，每个组都按它们在配置文件中出现的顺序被依次处理，而<Directory>（上面的第 1 组），会按顺序由短到长被依次处理。例如：<Directory /var/web/dir>会先于<Directory /var/web/dir/subdir>被处理。如果有多个指向同一个目录的<Directory>段，则按它们在配置文件中的顺序被依次处理。用 Include 指令包含进来的配置被视为按原样插入到 Include 指令的位置。

位于<VirtualHost>容器中的配置段在外部对应的段处理完毕以后再处理，这样就允许虚拟主机覆盖主服务器的设置。

当请求是由 `mod_proxy` 处理的时候，`<Proxy>` 容器将会在处理顺序中取代 `<Directory>` 容器的位置。也就是说，后面的段覆盖前面的相应的段。

3.2.3 Apache 2.2 的模块说明

为了使大家清楚 Apache 2.2 版本程序中所包括的各种类型模块及相关用途，本节将以列表的形式进行简要说明，如表 3-1 所示。通过这些模块的功能介绍我们就可以有选择地在 `httpd.conf` 配置文件中加载相应模块。

表 3-1 Apache 2.2 功能模块

模 块	功 能 说 明
core	Apache HTTP 服务器核心模块，始终有效
mpm_common	多个多路处理模块（MPM）实现的公共指令
beos	专门针对 Be 公司开发的 BeOS 多媒体操作系统优化后的 MPM
event	标准 workerMPM 的实验性变种模块
mpm_netware	专为 Novell NetWare 服务器系统优化的 MPM 模块
mpmt_os2	专门针对 OS/2 优化过的混合多进程多线程 MPM
prefork	非线程型的、预派生的 MPM，是 UNIX 系统平台上默认的 MPM
mpm_winnt	专为 Windows NT/2000/XP/2003 系列系统优化的 MPM
worker	线程型的 MPM，实现了一个混合的多线程多处理 MPM，允许一个子进程中包含多个线程
mod_actions	基于媒体类型或请求方法，为执行 CGI 脚本而提供的模块
mod_alias	提供从文件系统的不同部分到文档树的映射和 URL 重定向
mod_asis	发送自己包含 HTTP 头内容的文件
mod_auth_basic	使用基本认证
mod_auth_digest	使用 MD5 摘要认证（更安全，但是只有最新的浏览器才支持）
mod_authn_alias	基于实际认证支持者创建扩展的认证支持者，并为它起一个别名以便于引用
mod_authn_anon	提供匿名用户认证支持
mod_authn_dbd	使用 SQL 数据库为认证提供支持
mod_authn_dbm	使用 DBM 数据库为认证提供支持
mod_authn_default	在未正确配置认证模块的情况下简单拒绝一切认证信息
mod_authn_file	使用纯文本文件为认证提供支持
mod_authnz_ldap	允许使用一个 LDAP 目录存储用户名和密码数据库来执行基本认证和授权
mod_authz_dbm	使用 DBM 数据库文件为组提供授权支持
mod_authz_default	在未正确配置授权支持模块的情况下简单拒绝一切授权请求
mod_authz_groupfile	使用纯文本文件为组提供授权支持
mod_authz_host	供基于主机名、IP 地址、请求特征的访问控制
mod_authz_owner	基于文件的所有者进行授权
mod_authz_user	基于每个用户提供授权支持
mod_autoindex	自动对目录中的内容生成列表，类似于“ls”或“dir”命令
mod_cache	基于 URI 键的内容动态缓冲（内存或磁盘）
mod_cern_meta	允许 Apache 使用 CERN httpd 源文件，从而可以在发送文件时对头进行修改

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

138 网管员必读——网络应用（第2版）

（续表）

模 块	功 能 说 明
mod_cgi	在非线程型 MPM（prefork）上提供对 CGI 脚本执行的支持
mod_cgid	在线程型 MPM（worker）上用一个外部 CGI 守护进程执行 CGI 脚本
mod_charset_lite	允许对界面进行字符集转换
mod_dav	允许 Apache 提供 DAV 协议支持
mod_dav_fs	为 mod_dav 模块指令访问服务器上的文件系统提供支持
mod_dav_lock	为 mod_dav 模块指令锁定服务器上的文件提供支持
mod_dbd	管理 SQL 数据库连接，为需要数据库功能的模块提供支持
mod_deflate	压缩发送给客户端的内容
mod_dir	指定目录索引文件以及为目录提供“斜杠”（/）重定向
mod_disk_cache	基于磁盘的缓冲管理器
mod_dumpio	将所有 I/O 操作转储到错误日志中
mod_echo	一个很简单的协议演示模块
mod_env	允许 Apache 修改或清除传送到 CGI 脚本和 SSI 界面的环境变量
mod_example	一个很简单的 Apache 模块 API 演示模块
mod_expires	通过配置文件控制 HTTP 的“Expires:”和“Cache-Control:”头内容
mod_ext_filter	使用外部程序作为过滤器
mod_file_cache	提供文件描述符缓存支持，从而提高 Apache 性能
mod_filter	根据上下文实际情况对输出过滤器进行动态配置
mod_headers	允许通过配置文件控制任意的 HTTP 请求和应答头信息
mod_ident	实现 RFC1413 规定的 ident 查找
mod_imagemap	处理服务器端图像映射
mod_include	实现服务端包含文档（SSI）处理
mod_info	生成 Apache 配置情况的 Web 界面
mod_isapi	仅限于在 Windows 平台上实现 ISAPI 扩展
mod_ldap	为其他 LDAP 模块提供 LDAP 连接池和结果缓冲服务
mod_log_config	允许记录日志和定制日志文件格式
mod_log_forensic	实现“对比日志”，即在请求被处理之前和处理完成之后进行两次记录
mod_logio	对每个请求的输入/输出字节数以及 HTTP 头进行日志记录
mod_mem_cache	基于内存的缓冲管理器
mod_mime	根据文件扩展名决定应答的行为（处理器/过滤器）和内容（MIME 类型/语言/字符集/编码）
mod_mime_magic	通过读取部分文件内容自动猜测文件的 MIME 类型
mod_negotiation	提供内容协商支持
mod_nw_ssl	仅限于在 NetWare 平台上实现 SSL 加密支持
mod_proxy	提供 HTTP/1.1 的代理/网关功能支持
mod_proxy_ajp	mod_proxy 的扩展，提供 Apache JServ Protocol 支持
mod_proxy_balancer	mod_proxy 的扩展，提供负载均衡支持
mod_proxy_connect	mod_proxy 的扩展，提供对处理 HTTP CONNECT 方法的支持
mod_proxy_ftp	mod_proxy 的 FTP 支持模块
mod_proxy_http	mod_proxy 的 HTTP 支持模块

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(续表)	
模 块	功 能 说 明
mod_rewrite	一个基于一定规则的实时重写 URL 请求的引擎
mod_setenvif	根据客户端请求头字段设置环境变量
mod_so	允许运行时加载 DSO 模块
mod_speling	自动纠正 URL 中的拼写错误
mod_ssl	使用安全套接字层 (SSL) 和传输层安全 (TLS) 协议实现高强度加密传输
mod_status	生成描述服务器状态的 Web 界面
mod_suexec	使用与调用 Web 服务器用户的不同身份来运行 CGI 和 SSI 程序
mod_unique_id	为每个请求生成唯一的标识以便跟踪
mod_userdir	允许用户从自己的主目录中提供界面 (使用 “/~username”)
mod_usertrack	使用 Session 跟踪用户 (会发送很多 Cookie)，以记录用户的点击流
mod_version	提供基于版本的配置段支持
mod_vhost_alias	提供大批量虚拟主机的动态配置支持



workerMPM 使用多个子进程，每个子进程中又有多个线程。每个线程处理一个请求。该 MPM 通常对高流量的服务器是一个不错的选择。

3.2.4 指令术语

在正式介绍配置文件中所使用的指令之前，本节先对下节用于描述 Apache 配置指令的术语加以说明。这对于阅读有关 Apache 帮助文件是非常有用的。

1. 语法规则

语法规则指相应指令在配置文件中使用的形式 (随指令的不同而不同)，具体将在介绍相应指令时说明。指令后面一般可以跟一个或多个以空格分隔的参数。如果参数中有空格，则必须用双引号括起来，用方括号括起来的是可选参数。如果一个参数可以取多个值，则各个可能的值用 “|” 分隔。使用可变参数个数的指令以 “...” 符号结尾，以表示最后一个参数可以重复。

指令的参数类型非常多，以下列出常用的部分。

1) URL

一个完整 URL 包括类型、主机名和可选路径名的统一资源引用名，如 “http://www.example.com/path/to/file.html”。

2) URL-path

URL 中类型和主机名之后的部分，如 “/path/to/file.html” 是表示资源在网络空间 (而不是文件系统) 中的位置。

3) file-path

文件在本地文件系统中相对于根目录的路径，如 “Program Files/Apache Software Foundation/Apache2.2/htdocs/path/to/file.html”。除非以斜杠 (/) 开头，否则将被视为相对于 ServerAdministrators (服务器根目录，在 Windows 平台中为 “Apache 2.2”) 的相对路径。

140 网管员必读——网络应用（第2版）

4) directory-path

目录在本地文件系统中相对于根目录的路径，如“Program Files/Apache Software Foundation/Apache2.2/htdocs/path/to/”。

5) filename

不带路径信息的文件名，如“file.html”。

6) Regex

Perl 兼容的正则表达式，是对文本匹配模式的描述。指令的定义中会说明应该使用什么 Regex。



正则表达式（Regular Expression, Regex）是一种对模式的文字表述，比如，“所有以字母 A 开头的单词”，“每个 10 位的电话号码”，还可以是“每个包含两个逗号，而且没有大写字母 Q 的句子”等。正则表达式在 Apache 中非常有用，可以非常灵活地对一组文件或资源应用某种属性，例如，任何“images”目录下的“.gif”和“.jpg”文件可以表述为“/images/.*(jpg|gif)\$”。Apache 使用的是由 PCRE 库提供的 Perl 兼容的正则表达式。

7) extension

一般是指 filename 中最后一个“.”号后面的部分。不过，Apache 可以辨认文件的多个 extension，如果 filename 中含有多个“.”，则第一个“.”后面由每个“.”分隔开的部分都是此文件的 extension。比如“file.html.en”有两个 extension：“.html”和“.en”。在 Apache 指令中指定 extension 时，可以有也可以没有前导的“.”，而且不区分大小写。

8) MIME-type

一种用一个主格式类型和一个副格式类型并用斜杠分隔的描述文件格式的方法，如“text/html”。

9) env-variable

这是 Apache 配置过程中定义的环境变量的名称。注意，它不一定与操作系统中的环境变量相同。

2. 默认值

“默认值”就是没有在配置中明确指定，由 Apache 服务器在安装后自动选择的那个特定值。如果该指令有默认值，会在介绍相应指令时说明。如果没有，则会指明是“None”。

3. 作用域

它表示该指令出现在配置文件的什么位置才是合法的。它是一个用顿号分隔的一个或多个下列值的列表，如：

1) server config

说明该指令可以用于服务器配置文件（httpd.conf），但不能用于任何<VirtualHost>（虚拟主机）或<Directory>段及.htaccess 文件中。

2) virtual host

说明该指令可以用于服务器配置文件的<VirtualHost>段中。

3) directory

说明该指令可以用于服务器配置文件<Directory>、<Location>、<Files>、<Proxy>段中，

并服从配置段一文的限制。

4) .htaccess

说明该指令可以用于针对单个目录及其子目录的.htaccess 文件中。它可能会因 overrides 的设置而不起作用。指令应该仅仅出现在允许出现的作用域中，否则会产生配置错误，并导致服务器不能正确处理请求，或者根本不能启动。

指令的有效位置，事实上是其所有列出的作用域逻辑或的结果。也就是如果一个指令被标为“server config, .htaccess”则可以用于 httpd.conf 和.htaccess，但不能用于任何<Directory>或<VirtualHost>容器。

5) 覆盖项

该属性表示要使.htaccess 文件中的该指令有效必须激活的配置覆盖项。如果一个指令的作用域不包含.htaccess，则无此内容。

AllowOverride 指令使覆盖生效，并作用于一个特定的范围（比如一个目录）及其下分支，除非又被其下层中其他的 AllowOverride 指令所修改。指令的说明中同时列出了其可能的覆盖项。

4. 状态

状态代表了此指令与 Apache 服务器结合的紧密程度。也就是说，有可能需要重新编译服务器以获得一个指令的功能。其可能的值如下。

1) Core

Apache 服务器最核心的部分，始终有效。

2) MPM

由一个多路处理模块提供，此类指令仅仅在使用了指令定义中模块一行所列的 MPM 之后才有效。

3) Base

由默认编译进服务器的一个 Apache 标准模块提供，一般总是有效的，除非你刻意在编译时从配置中删除此模块。

4) Extension

由一个默认不被编译进服务器的模块提供。要激活此指令并使用其功能，需要修改服务器编译时配置并重新编译 Apache。

5) Experimental

由一个一般来说默认不被编译进服务器的模块提供，并且需要自己承担使用中的风险。对此指令提供文档是为了保持完整性，而并不一定有技术支持。提供此指令的模块，是否默认被编译进入服务器都有可能，这说明界面的顶部注明了模块的有效性。

5. 模块

模块用于指出对所对应的指令提供支持的模块列表。

6. 兼容性

如果对应指令不是原始 Apache 2.0 以上版本的一部分，此处会写明此指令应该被使用于哪个版本；另外，如果此指令在特定平台上有功能限制，此处会有详细说明。

3.2.5 Apache 2.2 核心指令

上节介绍了 Apache 2.2 版本的主要功能模块，其中就包括其核心模块。它是整个服务器系统中的功能核心，始终有效。因篇幅原因，下面仅介绍 Apache 2.2 核心模块中的一部分主要指令，不过大家可以从这些介绍的指令中学到反比例的使用方法。

1. AcceptFilter 指令

该指令是用来根据协议类型对监听 Socket 进行优化，其基本前提是内核在数据接收完毕或一个完整的 HTTP 请求缓冲完成前不向服务器进程发送 Socket。其语法格式为：AcceptFilter protocol accept_filter。其作用域为 server config，且仅在 Apache 2.1.5 以后的版本中可用。

目前仅支持 FreeBSD 的接收过滤器（Accept Filter）和 Linux 的更原始的（more primitive）TCP_DEFER_ACCEPT。

FreeBSD 上的默认值是：AcceptFilter http httpready 和 AcceptFilter https dataready。

httpready 接收过滤器（Accept Filter）在内核级别缓冲整个 HTTP 请求。一旦一个请求体被完整接收，内核将把它发送给服务器。因为 HTTP 请求已经被加密了，所以只使用了 accf_data (9) 过滤器。

Linux 上的默认值是：AcceptFilter http data 和 AcceptFilter https data。

Linux 的 TCP_DEFER_ACCEPT 并不支持对 HTTP 请求进行缓冲。除 none 之外的任何值都将在监听程序上启用 TCP_DEFER_ACCEPT。

使用 none 将会为那个协议禁用接收过滤器（Accept Filter）。这对于像 ntp 这样需要服务器先发送数据的协议很有用处，其语法格式为：AcceptFilter ntp none。

2. AcceptPathInfo 指令

该指令是用来决定是否接受附带多余路径名信息的请求。这个多余的路径名信息可以当做 PATH_INFO 环境变量传递给脚本。

其语法格式为：AcceptPathInfo On|Off|Default。

其作用域为 server config、virtual host、directory 和 htaccess，默认值为 AcceptPathInfo Default，仅在 Apache 2.0.30 及以后的版本中可用。

比如，假设 /test/ 所指向的目录下只包括一个文件：here.html，那么对 /test/here.html/more 和 /test/nother.html/more 的请求都会将 PATH_INFO 环境变量设为 “more”。

当 AcceptPathInfo 指令取值 “Off” 时，仅当一个请求映射到一个真实存在的路径时，才会被接受。这样，如上述 /test/here.html/more 这样在真实文件名后跟随一个路径名的请求将会返回一个 “404 NOT FOUND” 错误。

当取值为 “On” 时，只要前导路径可以映射到一个真实存在的文件中，就可以接受该请求。这样，只要上述 “/test/here.html” 能够映射到一个有效的文件，那么 /test/here.html/more 的请求就会被接受。

当取值为 “Default” 时，是否接受附带多余路径名信息的请求由其对应的处理器来决定。对应普通文本的核心处理器默认会拒绝 PATH_INFO。而用于伺服脚本的处理器，比如 cgi-script 和 isapi-isa，默认会接受 PATH_INFO。

AcceptPathInfo 指令存在的首要目的就是允许你覆盖处理器关于是否接受 PATH_INFO 的

默认设置，这种覆盖是很必要的。比如说，当你使用了类似 INCLUDES 这样的过滤器来根据 PATH_INFO 产生内容时。核心处理器通常会拒绝这样的请求，而你就可以用下述的配置使这样的脚本成为可能：

```
<Files "mypaths.shtml">
  Options +Includes
  SetOutputFilter INCLUDES
  AcceptPathInfo On
</Files>
```

3. AccessFileName 指令

该指令用来定义分布式配置文件的名字。如果为某个目录启用了分布式配置文件功能，那么在向客户端返回其中的文档时，服务器将在这个文档所在的各级目录中查找此配置文件。其语法格式为：AccessFileName filename。比如，AccessFileName.acl。在返回文档 /usr/local/web/index.html 之前，服务器会为此指令读取 /.acl、/usr/.acl、/usr/local/.acl、/usr/local/web/.acl。除非此功能已被如下配置所禁用：

```
<Directory />
  AllowOverride None
</Directory>
```

其作用域为 server config 和 virtual host，默认值为：AccessFileName .htaccess。

4. AddDefaultCharset 指令

该指令当应答内容是 text（文本）/plain（图片）或 text/html（网页）时，在 HTTP 应答头中加入默认字符集。其语法格式为：AddDefaultCharset On|Off|charset。

其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：AddDefaultCharset Off。

理论上这将覆盖在文档体中通过<meta>标签指定的字符集，但是实际的行为通常取决于用户浏览器的设置。AddDefaultCharset Off 将会禁用此功能。AddDefaultCharset On 将启用 Apache 内部的默认字符集 iso-8859-1。也可以指定使用在 IANA 注册过的字符集名字中的另外一个 charset。比如说：

```
AddDefaultCharset utf-8
```

AddDefaultCharset 只在如下情况下使用：所有文本资源都使用同一种确定的字符集，且分别标记他们的字符集非常麻烦。一个这样的例子是向包含动态内容的资源中添加字符集参数（比如，先前遗留的 CGI 脚本），这样可能会因为在输出中包含用户提供的数据而导致跨站点脚本攻击。但是请注意：更好的解决办法是修改或删除这些脚本，因为设置了默认的字符集以后将会使得浏览器的字符集自动探测功能失效。

5. AddOutputFilterByType 指令

该指令对特定的 MIME 类型指定输出过滤器。其语法格式为：AddOutputFilterByType filter[;filter...] MIME-type [MIME-type]...。

其作用域为：server config、virtual host、directory 和 .htaccess。Apache 2.0.33 以后的版本可用，但在 Apache 2.1 以后的版本反对使用。



在某些情况下，用 `AddOutputFilterByType` 来指定过滤器会遭受部分或完全的失败。比如，如果 MIME 类型不能确定，那么将不会有过滤器加于其上，从而使之回到 `DefaultType` 的设置。甚至当 `DefaultType` 与其相同的时候也是这样。然而，如果想确认对某些资源相关的内容类型使用了过滤器，可以使用诸如 `AddType` 或 `ForceType` 这样的办法。在一个（non-nph）CGI 脚本中设定内容类型也很安全。

由类型决定的输出过滤器永远不会作用于来自代理的请求。

6. AllowEncodedSlashes 指令

该指令用来确定是否允许 URL 中使用经过编码的路径分割符。在默认情况下，这些 URL 将被一个包含“404 NOT FOUND”（未找到）错误的应答拒绝。

其语法格式为：`AllowEncodedSlashes On|Off`。

其作用域为：`server config` 和 `virtual host`。默认值为：`AllowEncodedSlashes Off`。不过仅在 Apache 2.0.46 及以后的版本中可用。

`AllowEncodedSlashes On` 通常和 `PATH_INFO` 配合使用。

7. AllowOverride 指令

该指令用来确定允许存在于 `.htaccess` 文件中的指令类型。当服务器发现一个 `.htaccess` 文件（由 `AccessFileName` 指定）时，它需要知道在这个文件中声明的哪些指令能覆盖在此之前指定的配置指令。

其语法格式为：`AllowOverride All|None|directive-type [directive-type] ...`

其作用域为：`directory`，仅允许存在于 `<Directory>` 配置段中。默认值为：`AllowOverride All`。

`AllowOverride` 仅在不包含正则表达式的 `<Directory>` 配置段中才是有效的。在 `<Location>`、`<DirectoryMatch>`、`<Files>` 配置段中都是无效的。

如果此指令被设置为 `None`，那么 `.htaccess` 文件将被完全忽略。事实上，服务器根本不会读取 `.htaccess` 文件。当此指令设置为 `All` 时，所有具有“`.htaccess`”作用域的指令都允许出现在 `.htaccess` 文件中。

上述语法格式中的“`directive-type`”可以是下列各组指令之一。

1) AuthConfig

`AuthConfig` 允许使用与认证授权相关的指令（`AuthDBMGroupFile`、`AuthDBMUserFile`、`AuthGroupFile`、`AuthName`、`AuthType`、`AuthUserFile` 和 `Require` 等）。

2) FileInfo

`FileInfo` 允许使用控制文档类型的指令（`DefaultType`、`ErrorDocument`、`ForceType`、`LanguagePriority`、`SetHandler`、`SetInputFilter`、`SetOutputFilter`、`mod_mime` 中的 `Add*` 和 `Remove*` 指令等）、控制文档源数据的指令（`Header`、`RequestHeader`、`SetEnvIf`、`SetEnvIfNoCase`、`BrowserMatch`、`CookieExpires`、`CookieDomain`、`CookieStyle`、`CookieTracking`、`CookieName`）、`mod_rewrite` 中的指令（`RewriteEngine`、`RewriteOptions`、`RewriteBase`、`RewriteCond`、`RewriteRule`）和 `mod_actions` 中的 `Action` 指令。

3) Indexes

`Indexes` 允许使用控制目录索引的指令（`AddDescription`、`AddIcon`、`AddIconByEncoding`、

AddIconByType、DefaultIcon、DirectoryIndex、FancyIndexing、HeaderName、IndexIgnore、IndexOptions、ReadmeName 等)。

4) Limit

Limit 允许使用控制主机访问的指令 (Allow、Deny、Order)。

5) Options[=Option,...]

Options[=Option,...]允许使用控制指定目录功能的指令 (Options 和 XBitHack)。可以在等号后面附加一个用逗号分隔的 (无空格的) Options 选项列表，用来控制允许 Options 指令使用哪些选项。

例如，以下指令只允许在.htaccess 中使用 AuthConfig 和 Indexes 组的指令。

AllowOverride AuthConfig Indexes

不在这两组中的指令将会导致服务器产生一个内部错误。

8. AuthName 指令

该指令用于设置 HTTP 认证的授权域。其语法格式为：AuthName auth-domain。作用域为：directory 和.htaccess。

此指令为目录的授权域设置名字。此域将发送给客户端以使用户了解应当发送哪个用户名和密码。AuthName 指令带有一个参数。如果域的名字中包含空格，则必须用引号引起来。AuthName 指令必须与 AuthType 和 Require 指令，以及诸如 AuthUserFile 和 AuthGroupFile 这样的指令一起工作。

例如：AuthName “Top Secret”。

提供给 AuthName 的字符串将出现在大多数浏览器提供的密码对话框中。

9. AuthType 指令

该指令用于设置用户认证类型。其语法格式为：AuthType Basic|Digest，其作用域为：directory 和.htaccess。

此指令目前只实现了 Basic (mod_auth_basic) 和 Digest (mod_auth_digest)。

要实现认证，还必须同时与 AuthName 和 Require 指令一起使用。另外，服务器还必须包含一个认证支持模块 (比如 mod_authn_file) 和一个授权支持模块 (比如 mod_authz_user)。

10. CGIMapExtension 指令

该指令用于定位 CGI 脚本解释器。其语法格式为：CGIMapExtension cgi-path .extension。其作用域为：directory 和.htaccess。

11. ContentDigest 指令

该指令允许生成 Content-MD5 应答头。其语法格式为：ContentDigest On|Off，作用域为：server config、virtual host、directory 和.htaccess，默认值为：ContentDigest Off。

此指令遵照 RFC1854 和 RFC2068 协议的定义，启用了 Content-MD5 应答头的生成。MD5 是一种为不定长度的数据计算出一个“消息摘要” (有时也称为“指纹”) 的算法。并且保证数据中的任何变化都会反应在消息摘要的变化中。Content-MD5 头提供了一种端到端的针对整个消息体的信息完整性检查方法。代理或者客户端会检查此头以侦测在传输过程中，消息体是否产生了意外的改变。一个头的例子如下：

Content-MD5: AuLb7Dp1rqtRtxz2m9kRpA==



注意

因为对每个请求都要进行消息摘要的运算（没有对其值进行缓存），所以这会对服务器造成性能方面的影响。Content-MD5 仅为 Apache 核心伺服的文档进行发送，而对于由模块处理的文档则不予理会。比如说 SSI 文档、CGI 脚本的输出、字节范围的应答都不包括这个头。

12. DefaultType 指令

该指令用于服务器无法由其他方法确定内容类型时，发送默认的 MIME 内容类型。其语法格式为：DefaultType MIME-type。其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：DefaultType text/plain。

有时会发生这样的事：服务器会被要求提供一个文档，而这个文档的类型无法由它的 MIME 类型映射所决定。而服务器必须通知客户端其文档的内容类型，所以当未知类型出现时，将会使用 DefaultType。例如：

DefaultType image/gif

这样的配置对于里面有很多 gif 格式的图片而有些在文件名中缺少 .gif 扩展名的目录非常合适。



注意

与 ForceType 指令的不同之处在于：此指令仅提供了默认的 MIME 类型。所有其他 MIME 类型的定义，包括文件的扩展名，或其他可以标识媒体类型的方法都会覆盖此默认值。

13. <Directory> 指令

该指令用来封装一组指令，使之仅对文件空间中的某个目录及其子目录生效。其语法格式为：<Directory directory-path> ... </Directory>。其作用域为：server config 和 virtual host。

任何可以在“directory”作用域中使用的指令都可以使用。Directory-path 可以是一个目录的完整路径，或是包含了 UNIX shell 匹配语法的通配符字符串。在通配符字符串中，“?”匹配任何单个的字符，“*”匹配任何字符序列。你也可以使用“[]”来确定字符范围。以上通配符都不能匹配“/”字符。所以<Directory */public_html>将无法匹配/home/user/public_html，但<Directory /home/*/public_html>能够正确匹配。比如说：

```
<Directory /usr/local/httpd/htdocs>
Options Indexes FollowSymLinks
</Directory>
```



注意

使用 directory-path 参数时，必须与 Apache 用于访问文件的文件系统路径保持一致。赋予特定<Directory>的指令将无法对通过不同路径指向的同一个目录文件生效，比如说通过另外一个符号连接生成的路径。

扩展的正则表达式也可以通过附加一个“~”字符来使用。比如：

```
<Directory ~ "/^www/ (.+)" *[0-9]{3}" >
```

以上语句将匹配/www/下所有由3个数字组成的目录。

如果有多个（非正则表达式）<Directory>配置段符合包含某文档的目录（或其父目录），那么指令将以短目录优先的规则进行应用。并包含.htaccess 文件中的指令。比如说：

```
<Directory />
    AllowOverride None
</Directory>

<Directory /home/>
    AllowOverride FileInfo
</Directory>
```

访问文档/home/web/dir/doc.html 的步骤如下：

- （1）应用指令 AllowOverride None（禁用.htaccess 文件）。
- （2）应用指令 AllowOverride FileInfo（针对/home 目录）。

（3）按顺序应用所有/home/.htaccess、/home/web/.htaccess、/home/web/dir/.htaccess 中的 FileInfo 组指令。

正则表达式将在所有普通配置段之后予以考虑。所有的正则表达式将根据它们出现在配置文件中的顺序进行应用。比如说，以下配置：

```
<Directory ~ abc$>
# .....
</Directory>
```

正则表达式配置段将在所有普通的<Directory>和.htaccess 文件应用之后才予以考虑。所以正则表达式将匹配/home/abc/public_html/abc 并予以应用。



Apache 对<Directory/>的默认访问权限为“Allow from All”。这意味着 Apache 将伺服任何通过 URL 映射的文件。建议将这个配置做如下屏蔽：

```
<Directory />
    Order Deny,Allow
    Deny from All
</Directory>
```

然后在你想要使之被访问的目录中覆盖此配置。

一般来说，<Directory>指令只会出现在 httpd.conf 文件中，但它们也可能出现在任何其他配置文件中。<Directory>指令不可被嵌套使用，也不能出现在<Limit>或<LimitExcept>配置段中。

14. <DirectoryMatch>指令

该指令用来封装一些指令，并作用于文件系统中匹配正则表达式的所有目录及其子目录。其语法格式为：<DirectoryMatch regex> ... </DirectoryMatch>。其作用域为：server config 和 virtual host。

<DirectoryMatch>和</DirectoryMatch>用于封装一组指令。与<Directory>类似，此指令将仅作用于指定名字的目录及其子目录。然而，它可以接受一个正则表达式作为参数。比如说：

```
<DirectoryMatch "^/www/(.+/*[0-9]{3})" # 匹配/www/目录下所有由3个数字组成的目录。
```

148 网管员必读——网络应用（第2版）

15. DocumentAdministrators 指令

该指令用来指定组成网络上可见的主文档树的根目录，也就是网站根目录。其语法格式为：DocumentAdministrators directory-path。其作用域为：server config 和 virtual host，默认值为：DocumentAdministrators /program Files/Apache Software Foundation/apache2.2/htdocs。

此指令设置了 httpd 伺服的目录。在没有使用类似 Alias 这样的指令的情况下，服务器会将请求中的 URL 附加到 DocumentAdministrators 后面以构成指向文档的路径。例如说：

```
DocumentAdministrators /usr/web
```

于是对 `http://www.my.host.com/index.html` 的访问就会指向 `/usr/web/index.html`。如果 `directory-path` 不是绝对路径，则被假定为是相对于 `ServerAdministrators` 的路径。

指定 DocumentAdministrators 时不应包括最后的 “/” 符号。

16. EnableMMAP 指令

该指令用于在传送中使用内存映射（memory-mapping）来读取文件。其语法格式为：EnableMMAP On|Off。其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：EnableMMAP On。

此指令指示 httpd 在递送中如果需要读取一个文件的内容，它是否可以使用内存映射。当处理一个需要访问文件中的数据请求时，比如说当递送一个使用 `mod_include` 进行服务器端分析的文件时，如果操作系统支持，那么 Apache 将默认使用内存映射。

这种内存映射有时会使性能提高，但在某些情况下，可能会需要禁用内存映射以避免一些操作系统的问题：在一些多处理器的系统上，内存映射会降低一些 httpd 的性能。在挂载了 NFS（网络文件系统）的 DocumentAdministrators 上，若已经将一个文件进行了内存映射，则删除或截断这个文件会造成 httpd 因为分段故障而崩溃。

在可能遇到这些问题的服务器配置过程中，应当使用下面的命令来禁用内存映射：

```
EnableMMAP Off
```

对于挂载了 NFS 的文件夹，可以单独指定禁用内存映射：

```
<Directory "/path-to-nfs-files"> EnableMMAP Off </Directory>
```

17. EnableSendfile 指令

该指令用来使用操作系统内核的 Sendfile 支持来将文件发送到客户端。其语法格式为：EnableSendfile On|Off。其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：EnableSendfile On。但这个指令仅在 Apache 2.0.44 及以后的版本中可用。

这个指令控制 httpd 是否可以使用操作系统内核的 Sendfile 支持来将文件发送到客户端。在默认情况下，当处理一个请求并不需要访问文件内部的数据时（比如发送一个静态的文件内容），如果操作系统支持，Apache 将使用 Sendfile 将文件内容直接发送到客户端而并不读取文件。

这个 Sendfile 机制避免了分开的读和写操作及缓冲区分配，但是在一些平台或者一些文件系统中，最好禁止这个特性来避免一些问题。

一些平台可能会由编译系统检测不到的有缺陷的 Sendfile 支持，特别是将在其他平台上使用交叉编译得到的二进制文件运行于当前对 Sendfile 支持有缺陷的平台时。

在 Linux 上启用 IPv6 时，使用 Sendfile 将会触发某些网卡上的 TCP 校验和卸载 bug。

当 Linux 运行在 Itanium 处理器上的时候，Sendfile 可能无法处理大于 2GB 的文件。

对于一个通过网络挂载了 NFS 文件系统的 DocumentAdministrators(比如 NFS 或 SMB)，内核可能无法可靠地通过自己的缓冲区服务于网络文件。

如果出现以上情况，应当采用下列语句禁用 Sendfile：

```
EnableSendfile Off
```

针对 NFS 或 SMB，这个指令可以被针对目录的设置覆盖，命令语句如下：

```
<Directory "/path-to-nfs-files"> EnableSendfile Off </Directory>
```

18. ErrorDocument 指令

该指令用于指定当遇到错误的时候服务器将给客户端什么样的应答。其语法格式为：

ErrorDocument error-code document。作用域为：server config、virtual host、directory 和.htaccess。

当遇到问题或错误的时候，Apache 能被配置为以下四种处理之一。

- 输出一个简单生硬的错误代码信息。
- 输出一个经过定制的信息。
- 重定向到一个本地的 URL-path 来处理这个问题（错误）。
- 重定向到一个外部的 URL 来处理这个问题（错误）。

默认会采取第一种方法，而第二、三和四种方法可以使用 ErrorDocument 指令后面跟随一个 HTTP 应答代码和一个 URL 信息来进行配置。Apache 有时会额外提供一些信息来描述所发生的问题或错误。

URL 可以由一个斜杠 (/) 开头来指示一个本地 URL（相对于 DocumentAdministrators），或是提供一个能被客户端解释的完整的 URL。此外还能提供一个可以被浏览器显示的消息。比如：

```
ErrorDocument 500 http://foo.example.com/cgi-bin/tester
ErrorDocument 404 /cgi-bin/bad_urls.pl
ErrorDocument 401 /subscription_info.html
ErrorDocument 403 "Sorry can't allow you access today"
```

另外，特殊的“default”值可以被用来指定使用 Apache 内置的、简单的硬编码消息。当不需要这个定制特性的时候，可以用“default”恢复 Apache 内置的、简单的硬编码消息，否则将继承一个已有的 ErrorDocument。



如果已经为 ErrorDocument 指定了一个外部的 URL（比如说，任何在开头指示了类似“http”这样的访问方法的字符串），Apache 将会向客户端发送一个重定向指令来告诉它在哪里找到这个文档，哪怕这个文档最后还是在这个服务器上。这里面包含着一些暗示：最重要的就是客户端无法接收到原始的错误状态代码，取而代之的是一个重定向状态代码。这将会使一些用状态代码来判断一个 URL 是否有效的 Web 处理器或其他客户端产生误解。另外，如果在“ErrorDocument 401”中使用了外部 URL，客户端将不会提示用户输入密码，因为它根本没收到这样一个 401 的状态代码。所以，如果想使用“ErrorDocument 401”指令，就必须指向一个本地的文档。

150 网管员必读——网络应用（第2版）

Microsoft Internet Explorer (MSIE) 在服务器端产生错误信息“很小”的时候会忽略它们，而用自己喜欢的错误信息进行取代（在 IIS 中也可以自定义错误信息）。这个大小的阈值根据错误类型而不同。但一般来说，如果你的错误信息的大小在 512B 以上，MSIE 就会显示这些服务器端产生的错误文档而不会屏蔽它们。

虽然大多数错误信息可以被改写，但是在有些情况下，将仍然使用某些内置的错误信息而不管 ErrorDocument 如何设置。特别是在检测到一个“畸形”请求的情况下，正常的请求处理过程将会被立即中断，并且立即返回一个内置的错误信息。这是为了防止某些不良请求可能导致的安全问题。

在 2.0 版以前，信息前面会用一个不配对的双引号作为前导标志。

19. FileETag 指令

该指令用以创建 ETag 应答头的文件的属性。其语法格式为：FileETag component ...。其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：FileETag INode MTime Size。

FileETag 指令配置了当文档是基于一个文件时用以创建 ETag（实体标签）应答头的文件的属性（ETag 的值用于进行缓冲管理以节约网络带宽）。在 Apache 1.3.22 及以前版本，ETag 的值总是由文件的 inode（索引节点）、大小、最后修改时间决定的。FileETag 指令可以选择这其中的哪些要素将被使用。主要关键字如下：

- Inode：文件的索引节点（inode）数。
- Mtime：文件的最后修改日期及时间。
- Size：文件的字节数。
- All：所有存在的域，等价于 FileETag INode MTime Size。
- None：如果一个文档是基于文件的，则不在应答中包含任何 ETag 头。

可以在 Inode、Mtime、Size 前加上“+”或“-”以改变由上层继承下来的默认值。任何没有上述前缀的关键字将立刻完全取消继承下来的设置。

如果一个目录的配置包含了“FileETag INode MTime Size”，而其一个子目录包含了“FileETag-Inode”，那么这个子目录的设置（并会被其下任何没有进行覆盖的子目录继承）将等价于“FileETag MTime Size”。

20. <Files>指令

该指令包含作用于匹配指定文件名的指令。其语法格式为：<Files filename> ... </Files>。其作用域为：server config、virtual host、directory 和 .htaccess。

<Files>指令提供了基于文件名的访问控制，类似于<Directory>和<Location>指令。它将配对一个</Files>指令。在此配置段中定义的指令将作用于其基本名称（不是完整的路径）与指定的文件名相符的对象。<Files>段将根据它们在配置文件中出现的顺序被处理：在<Directory>段和 .htaccess 文件被处理之后，但在<Location>段之前。请注意：<Files>能嵌入到<Directory>段中以限制它们作用的文件系统范围。

filename 参数应当是一个文件名或是一个包含通配符的字符串，其中“?”匹配任何单个字符，“*”匹配任何字符串序列。在“~”字符之后同样可以使用正则表达式。比如：

```
<Files ~". (gif|jpg|png)" $">
```

将匹配绝大部分常见的互联网图像格式。然而在 Apache 1.3 及其后续版本中，更推荐使用<FilesMatch>指令。

与<Directory>和<Location>配置段不同的是：<Files>配置段可用于.htaccess 文件当中。这将允许用户在文件层面上控制对它们自己文件的访问。

21. <FilesMatch>指令

该指令包含作用于与正则表达式匹配的文件名的指令。语法格式为：<FilesMatch regex> ... </FilesMatch>。其作用域为：server config、virtual host、directory 和.htaccess。

<FilesMatch>指令就像<Files>指令一样提供了针对文件名的访问控制。然而，它使用的是正则表达式。比如说：

```
<FilesMatch "\.(gif|jpeg|png)$"> # 匹配最常见的 Internet 图形文件格式。
```

22. ForceType 指令

该指令强制所有匹配的文件被作为指定的 MIME 类型进行伺服。其语法格式为：ForceType MIME-type|None。其作用域为：directory 和.htaccess。该指令是自 Apache 2.0 之后才从其他模块移动到核心模块中的。

当此指令放入.htaccess 文件或<Directory>或<Location>或<Files>配置段时，此指令强制所有匹配的文件被当做在 MIME-type 中指定的 Content-Type 来伺服。比如说，如果你有一个包含大量 gif 文件的目录，可又不想全都为它们加上“.gif”扩展名的话，可以输入以下语句：

```
ForceType image/gif
```

与 DefaultType 指令不同，此指令将覆盖所有的 mime 类型关联，包括标识文件类型的扩展名。可以通过使用“None”覆盖任何 ForceType 设置。如下语句段实现强制所有文件为 image/gif 类型：

```
<Location /images>
    ForceType image/gif
</Location>
```

但是正常的 MIME 类型关联是这样的：

```
<Location /images/mixed>
    ForceType None
</Location>
```

23. <IfDefine>指令

该指令用来封装一组只有在启动测试结果为真时才生效的指令。其语法格式为：<IfDefine [!]parameter-name> ... </IfDefine>。其作用域为：server config、virtual host、directory 和.htaccess。

<IfDefine test>...</IfDefine>配置段用于包含有条件的指令。<IfDefine>配置段中的指令仅当 test 结果为真时才进行处理。如果 test 为假，那么此配置段中的指令将会被忽略。

<IfDefine>配置段中的 test 可为 parameter-name 和!parameter-name 两种形式之一。

在第一种情况下，仅当 parameter-name 已经定义的情况下才对开始和结束标记之间的指令进行处理。第二种情况则截然相反，仅当 parameter-name 没有定义的情况下才进行指令的处理。parameter-name 是在服务启动时，通过 httpd 命令行的-Dparameter 的形式指定的。

152 网管员必读——网络应用（第2版）

<IfDefine>配置段是可以嵌套的，从而可以实现简单的多参数测试。比如说：

```
httpd -DReverseProxy ...
# httpd.conf
<IfDefine ReverseProxy>
    LoadModule rewrite_module modules/mod_rewrite.so
    LoadModule proxy_module modules/libproxy.so
</IfDefine>
```

24. <IfModule>指令

该指令用于封装指令，并根据指定的模块是否启用为条件而决定是否进行处理。其语法格式为：<IfModule [!]*module-file|module-identifier*> ... </IfModule>。其作用域为：server config、virtual host、directory 和 .htaccess。module-identifier 参数仅在 Apache 2.1 及以后的版本中可用。

<IfModule test>...</IfModule>配置段用于封装根据指定的模块是否启用而决定是否生效的指令。在<IfModule>配置段中的指令仅当 test 为真的时候才进行处理。如果 test 为假，那么所有其间的指令都将被忽略。

<IfModule>段中的 test 可为 module 和 !module 两种形式之一。在第一种情况下，起始和结束标记之间的指令仅当 module 被载入后才被执行，此模块可以为编译时静态链接核心的模块或是使用 LoadModule 指令动态载入的模块。第二种情况则相反，仅当 module 没有载入时才进行指令的处理。

module 可以是模块的标识符或者是编译模块时的文件名。比如，rewrite_module 就是一个模块标识符，而 mod_rewrite.c 则是编译模块时的文件名。如果模块包含多个源代码文件，应当使用包含 STANDARD20_MODULE_STUFF 字符串的那个。

<IfModule>配置段是可以嵌套的，从而可以实现简单的多模块测试。

此配置段主要用于需要根据某个特定的模块是否存在来决定是否使用某些配置的时候。指令一般都放在<IfModule>配置段中。

25. Include 指令

该指令用于在服务器配置文件中包含其他配置文件。其语法格式为：Include *file-path|directory-path*。其作用域为：server config、virtual host 和 directory。通配符仅在 Apache 2.0.41 及以后的版本中可用。

这个指令允许在服务器配置文件中加入其他配置文件。Shell 风格 (fnmatch()) 的通配符可以用于按照字母顺序一次包含多个文件。另外，如果 Include 指向了一个目录而不是一个文件，Apache 将读入该目录及其子目录下的所有文件，并依照字母顺序将这些文件作为配置文件进行解析。但是并不推荐这么做，因为偶尔会有临时文件在这个目录中生成，从而导致 httpd 启动失败。

文件的路径可以是一个完整的绝对路径（以一个斜杠开头），例如：

```
Include /Program Files/Apache Software Foundation/Apache2.2/conf/ssl.conf
Include /Program Files/Apache Software Foundation/Apache2.2/conf/vhosts/*.conf
```

或是相对于 ServerAdministrators 目录的相对路径：

```
Include conf/ssl.conf
Include conf/vhosts/*.conf
```

请确保包含的目录中不含有任何诸如编辑器临时文件等引起误导的文件，因为 Apache 会尝试读取它们并把其中的内容作为配置指令来处理，这样可能会导致启动过程的失败。运行 `apachectl configtest` 将会把配置检查时所使用的文件列出来以供参考。这将有助于检验配置中是否仅包含了希望出现的那些文件。

26. KeepAlive 指令

该指令用于启用 HTTP 持久链接功能。其语法格式为：`KeepAlive On|Off`。其作用域为：`server config` 和 `virtual host`，默认值为 `KeepAlive On`。

`Keep Alive` 扩展自 HTTP/1.0 和 HTTP/1.1 的持久链接特性。提供了长效的 HTTP 会话，用于在同一个 TCP 连接中进行多次请求。在某些情况下，这样的方式会对包含大量图片的 HTML 文档造成的延时起到 50% 的加速作用。在 Apache 1.2 版本以后，可以设置 `KeepAlive On` 以启用持久链接。

对于 HTTP/1.0 的客户端来说，仅当客户端指定使用的时候才会使用持久链接连接。此外，仅当能够预先知道传输的内容长度时，才会与 HTTP/1.0 的客户端建立持久链接连接。这意味着那些长度不定的内容，诸如 CGI 输出、SSI 界面，以及服务器端生成的目录列表等内容一般来说将无法使用与 HTTP/1.0 客户端建立的持久链接连接。而对于 HTTP/1.1 的客户端来说，如果没有进行特殊指定，持久链接将是默认的连接方式。如果客户端进行了请求，将使用分块编码以解决在持久链接里发送未知长度内容的问题。

27. KeepAliveTimeout 指令

该指令用于设置持久链接中服务器在两次请求之间等待的秒数。其语法格式为：`KeepAliveTimeout seconds`。其作用域为：`server config` 和 `virtual host`，默认值为：`KeepAliveTimeout 5`，也就是 5 秒。

Apache 在关闭持久连接前等待下一个请求的秒数。一旦收到一个请求，超时值将会被设置为 `Timeout` 指令指定的秒数。

对于高负荷服务器来说，`KeepAliveTimeout` 值较大可能会导致一些性能方面的问题：超时值越大，与空闲客户端保持连接的进程就越多。

28. <Limit>指令

该指令设置仅对指定的 HTTP 方法进行访问控制。其语法格式为：`<Limit method [method]...>...</Limit>`。其作用域为：`server config`、`virtual host`、`directory` 和 `htaccess`。

访问控制一般来说是对所有的访问方法都生效，这也是我们普遍希望达到的效果。一般情况下，访问控制指令不应该放入 `<Limit>` 段中。

`<Limit>` 指令的目的是限制访问控制的效果使其仅作用于某些 HTTP 方法。对于其他方法，`<Limit>` 括号中的访问限制将不起任何作用。下例中的访问控制仅作用于 POST、PUT、DELETE 方法，其他方法不受任何影响。

列出的方法名可为下列的一个或多个：GET、POST、PUT、DELETE、CONNECT、OPTIONS、PATCH、PROPFIND、PROPPATCH、MKCOL、COPY、MOVE、LOCK 和 UNLOCK。方法名是大小写敏感的。如果对 GET 进行了定义，它会同时作用于 HEAD 请求。TRACE 方法不能被限制。



注意

应当总是优先使用<LimitExcept>段来限制访问，而不是<Limit>段。因为<LimitExcept>段能够防范所有 HTTP 方法。

29. <LimitExcept>指令

该指令用于设置对除了指定方法以外的所有 HTTP 方法进行访问控制。其语法格式为：<LimitExcept method [method]...>...</LimitExcept>。其作用域为：server config、virtual host、directory 和 .htaccess。

<LimitExcept>用于封装一组访问控制指令，并将其作用于所有没有在参数中标出的 HTTP 方法。也就是说，与<Limit>相反，它用于控制标准、非标准及无法辨识的方法。

例如：

```
<LimitExcept POST GET>
    Require valid-user
</LimitExcept>
```

30. LimitRequestBody 指令

该指令用于限制客户端发送的 HTTP 请求体的最大字节长度。其语法格式为：LimitRequestBody Bytes。其作用域为：server config、virtual host、directory 和 .htaccess，默认值为：LimitRequestBody 0。

Bytes 参数在 0（意味着无限制）到 2 147 483 647B（2GB）间限制了请求体所允许的字节数。

LimitRequestBody 可以让用户在其作用范围内（整个服务器、特定目录、特定文件、特定位置）设置一个允许客户端发送的 HTTP 请求体的最大字节长度的限制。如果客户端的请求超出了这个限制，服务器会回应一个错误而不是伺服这个请求。一个普通请求的信息体在很大程度上取决于资源的自然属性和这个资源允许的方法。CGI 脚本经常用消息体把表单的信息传递给服务器。使用 PUT 方法至少会需要与服务器期望从这个资源得到的信息量差不多大小的值。

此指令给了服务器管理员更大的可控性以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。比如，如果允许文件上传到某个位置，而且希望能将上传文件的大小设置为 100KB，那么就可以使用下面的指令：

```
LimitRequestBody 102400
```

31. LimitRequestFields 指令

该指令用于限制接受客户端请求中 HTTP 请求头域的数量。其语法格式为：LimitRequestFields number。其作用域为：server config，默认值为：LimitRequestFields 100。

Number 参数是一个 0（意味着无限制）到 32 767 之间的整数。默认值为编译时的常量 DEFAULT_LIMIT_REQUEST_FIELDS（发布值为 100）。

LimitRequestFields 指令允许服务器管理员修改在一个 HTTP 请求中的请求头域的数量限制。服务器需要此值大于一个普通客户端请求中包含头域的数量。一个客户端请求头域的数量很少大于 20，但根据客户端的不同这个数字有很大的差别，经常取决于用户配置他们的浏览器扩展以支持更详细的内容协商。可选的 HTTP 扩展经常使用请求头域来实现。

这个指令给了服务器管理员更大的可控性以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。如果正常使用的客户端得到了服务器的错误应答，指出其在请求中发送了过多的头域，你应该适当地增大此值。

例如：

`LimitRequestFields 50`

32. LimitRequestFieldSize 指令

该指令用于限制客户端发送的请求头的字节数。其语法格式为：`LimitRequestFieldSize Bytes`。其作用域为：`server config`，默认值为：`LimitRequestFieldSize 8190`。

`Bytes` 参数指定了 HTTP 请求头允许的字节大小。

`LimitRequestFieldSize` 指令允许服务器管理员增加或减少 HTTP 请求头域大小的限制。一般来说，服务器需要此值足够大，以适应普通客户端的任何请求的头域大小。一个普通头域的大小对于不同的客户端来说是有很大差别的，一般与用户配置他们的浏览器以支持更多的内容协议密切相关。`SPNEGO` 的认证头最大可能达到 12 392 字节。

这个指令给了服务器管理员更大的可控性以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。

例如：

`LimitRequestFieldSize 4094`

一般情况下，请不要改变这个设置，而是保持其默认设置。

33. LimitRequestLine 指令

该指令用于限制接收客户端发送的 HTTP 请求行的字节数。其语法格式为：`LimitRequestLine Bytes`。其作用域为：`server config`，默认值为：`LimitRequestLine 8190`。

`Bytes` 参数将设置 HTTP 请求行的字节数限制。

`LimitRequestLine` 指令允许服务器管理员增加或减少客户端 HTTP 请求行允许大小的限制。因为请求行包括 HTTP 方法、URI、协议版本，所以 `LimitRequestLine` 指令会限制请求 URI 的长度。服务器会需要这个值足够大以装载它所有的资源名，包括可能在 GET 请求中所传递的查询部分的所有信息。

这个指令给了服务器管理员更大的可控性以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。

例如：

`LimitRequestLine 4094`

一般情况下，不需要改变此设置的默认值。

34. <Location>指令

该指令用于将封装的指令作用于匹配的 URL。其语法格式为：`<Location URL-path|URL> ... </Location>`。其作用域为：`server config` 和 `virtual host`。

`<Location>` 提供了基于 URL 的访问控制。与 `<Directory>` 指令类似，它也会启用一个以 `</Location>` 结尾的配置段。`<Location>` 配置段的处理位于 `<Directory>`、`.htaccess` 和 `<Files>` 容器之后，并依照在配置文件中出现的顺序进行处理。

156 网管员必读——网络应用（第2版）

<Location>配置段完全独立于文件系统之外操作。这有几个重要的后果，最重要的是<Location>不能用于针对文件系统的访问控制。因为可能会有几个不同的 URL 指向文件系统中的同一个文件，所以这样的控制常常会很容易绕过。

使用<Location>将指令应用于独立文件系统之外的内容。文件系统之内的内容请使用<Directory>和<Files>指令。不过，一个例外是<Location />，它可以方便地作用于所有 URL。

对所有的原始（非代理）请求来说，匹配的 URL 应该是具有“/path/”形式的 URL 路径，不包括访问方法、主机名、端口或查询字符串等。对于代理的请求，匹配的 URL 必须为“scheme://servername/path”的形式，而且必须包括前缀。

URL 可以用一个通配符字符串来处理。“?”匹配任何单个的字符，而“*”匹配所有字符序列，也可以附加“~”字符来表示正则表达式。例如：

```
<Location ~"/(extra|special)/data">
```

将匹配所有包含字符串“/extra/data”或“/special/data”的 URL。在 Apache 1.3 及其后续版本中，加入了一个新的推荐使用的<LocationMatch>指令，其功能与<Location>的正则表达式版本相同。

<Location>的功能在与 SetHandler 指令一起用时能发挥最大效能。比如启用状态请求，但仅对来自 foo.com 的用户有效，你可以这样使用：

```
<Location /status>
SetHandler server-status
Order Deny,Allow
Deny from all
Allow from .foo.com
</Location>
```



请注意语句中的“/”（斜杠）。斜杠字符根据它在 URL 中出现的位置不同有着特殊的意义。大家可能都已经习惯在文件系统中，多个连续的斜杠会被作为单一的斜杠处理（例如“/home///foo”与“/home/foo”相同）。但在 URL 里面，这样是行不通的。<LocationMatch>指令和正则表达式版本的<Location>要求你明确使用多重斜杠。比如：<LocationMatch ^/abc>将匹配请求“/abc”，但不会匹配请求“//abc”。而非正则表达式版本的<Location>指令在用于代理请求时，也有类似表现。但当非正则表达式版本的<Location>作用于非代理请求时，它会将多个毗邻的斜杠认做单个斜杠。比如，如果你指定了<Location /abc/def>，而请求是指向“/abc//def”的，那么它们就是匹配的。

35. LogLevel 指令

该指令用于控制错误日志的详细程度，也就是我们平常所说的日志事件类型的选择。其语法格式为：LogLevel level。其作用域为：server config, virtual host，默认值为：LogLevel warn。

LogLevel 用于调整记录在错误日志中的信息的详细程度。可以选择表 3-2 所示的 Level（依照重要性降序排列）。

表 3-2 日志 level

Level	描 述	日志记录示例
emerg	紧急（系统无法使用）	“Child cannot open lock file. Exiting”
alert	必须立即采取措施	“getpwuid: couldn't determine user name from uid”
crit	致命情况	“socket: Failed to get a socket, exiting child”
error	错误情况	“Premature end of script headers”
warn	警告情况	“child process 1234 did not exit, sending another SIGHUP”
notice	一般重要情况	“httpd: caught SIGBUS, attempting to dump core in ... ”
info	普通信息	“ Server seems busy, (you may need to increase StartServers, or Min/MaxSpareServers) ... ”
debug	调试信息	“Opening config file ... ”

当指定了某个级别时，所有级别高于它的信息也会被同时记录。比如，指定 LogLevel info，则所有 notice 和 warn 级别的信息也会被记录。

建议至少使用 crit 级别。

例如：

LogLevel notice



当错误日志是一个单独分开的正式文件的时候，notice 级别的消息总是会被记录下来，而不能被屏蔽。但是，当使用 syslog 来记录时就没有这个问题。

36. MaxKeepAliveRequests 指令

该指令用于设置一个持久链接中允许的最大请求数量。其语法格式为：MaxKeepAliveRequests number。其作用域为：server config 和 virtual host，默认值为：MaxKeepAliveRequests 100。

MaxKeepAliveRequests 指令限制了当启用 KeepAlive 时，每个连接允许的请求数量。如果将此值设为“0”，将不限制请求的数目。我们建议最好将此值设为一个比较大的值，以确保最优的服务器性能。

例如：

MaxKeepAliveRequests 500

37. NameVirtualHost 指令

该指令用于为一个基于域名的虚拟主机指定一个 IP 地址（和端口）。其语法格式为：NameVirtualHost addr[:port]。作用域为：server config。

如果要配置基于域名的虚拟主机，NameVirtualHost 指令就是必须的指令之一。

尽管 addr 参数可以使用主机名，但建议还是使用 IP 地址。例如：

NameVirtualHost 111.22.33.44

使用 NameVirtualHost 指令，可以指定一个基于域名的虚拟主机将使用哪个 IP 地址来接受请求。在一个防火墙或是其他代理接受了请求并把它转到服务器所在的另外一个 IP 地址上

158 网管员必读——网络应用（第2版）

的情况下，必须指定伺服请求的机器物理界面上的 IP 地址。如果多个地址使用了多个基于域名的虚拟主机，应该为每个地址使用这个指令。



“主服务器”和任何其他“_default_”服务器都不会伺服发送到 NameVirtualHost IP 地址的请求（除非指定了 NameVirtualHost，但没有为这个地址指定任何 VirtualHost）。

另外，还可以为基于域名的虚拟主机指定一个端口号。例如：

```
NameVirtualHost 111.22.33.44:8080
```

为了接受所有界面的请求，可以使用“*”通配符，例如：

```
NameVirtualHost *
```

<VirtualHost>指令的参数必须与 NameVirtualHost 指令的参数完全匹配。例如：

```
NameVirtualHost 1.2.3.4
<VirtualHost 1.2.3.4>
# ...
</VirtualHost>
```

38. Require 指令

该指令用于指定哪些认证用户允许访问该资源。其语法格式为：Require entity-name [entity-name] ...。其作用域为：directory 和 .htaccess。

这些限制由授权支持模块实现。只有指定的用户可以访问此目录。以下语句设置只有隶属于指定组的用户可以访问此目录。

```
Require group group-name [group-name] ...
```

以下语句设置所有有效用户都可以访问此目录。

```
Require valid-user
```

提供 Require 指令的授权支持模块有：mod_authz_user、mod_authz_groupfile、mod_authnz_ldap、mod_authz_dbm、mod_authz_owner。

Require 必须伴随 AuthName 和 AuthType 指令，以及诸如 AuthUserFile 和 AuthGroupFile 指令（用以定义用户和用户组）以确保其能够正确工作。例如：

```
AuthType Basic
AuthName "Restricted Resource"
AuthUserFile /web/users
AuthGroupFile /web/groups
Require group admin
```

使用这种方法提供的访问控制对所有方法都有效。这是一般情况下期望达到的效果。如果仅希望对某个特定的方法加以限制，而不涉及其他方法时，可以将 Require 语句放入<Limit>配置段中。

如果 Require 与 Allow 或 Deny 指令同时使用，那么这些指令之间的相互作用由 Satisfy 指令控制。

下面的例子展示了如何使用 `Satisfy` 指令在一个受保护的目录下的子目录中取消访问控制。使用这种方法必须十分小心，因为它取消了 `mod_authz_host` 实现的任何访问控制。

```
<Directory /path/to/protected/>
Require user david
</Directory>
<Directory /path/to/protected/unprotected> # 该目录下的所有认证和访问控制都被取消了
Satisfy Any
Allow from all
</Directory>
```

39. ServerAdmin 指令

该指令用于设置服务器返回给客户端的错误信息中包含的管理员邮件地址。其语法格式为：`ServerAdmin email-address|URL`。作用域为：`server config` 和 `virtual host`。

`ServerAdmin` 设置了在所有返回给客户端的错误信息中包含的管理员邮件地址。如果 `httpd` 不能将提供的参数识别为 `URL`，它就会假定它是一个 `email-address`，并在超链接中用在 `mailto:` 后面。推荐使用一个 `E-mail` 地址，因为许多 `CGI` 脚本是这样认为的。如果确实想使用 `URL`，一定要保证指向一个能够控制的服务器，否则用户将无法确保与你取得联系。

为这个目的专门设置一个邮箱是值得的，例如：

```
ServerAdmin www-admin@foo.example.com
```

40. ServerAlias 指令

该指令用于匹配一个基于域名的虚拟主机的别名。其语法格式为：`ServerAlias hostname [hostname] ...`。作用域为：`virtual host`。

`ServerAlias` 指令设定主机的别名，用于基于域名的虚拟主机。

```
<VirtualHost *>
    ServerName server.domain.com
    ServerAlias server server2.domain.com server2
    # ...
</VirtualHost>
```

41. ServerName 指令

该指令用于设置服务器辨识自己的主机名和端口号。其语法格式为：`ServerName fully-qualified-domain-name[:port]`。其作用域为：`server config`, `virtual host`。该指令在 2.0 版中，代替了 1.3 版的 `Port` 指令的功能。

`ServerName` 指令设置了服务器用于辨识自己的主机名和端口号。这主要用于创建重定向 `URL`。比如，一个放置 `Web` 服务器的主机名为 `simple.example.com`，但同时有一个 `DNS` 别名为 `www.example.com`。而你希望 `Web` 服务器更显著一点，可以使用如下的指令：

```
ServerName www.example.com:80
```

当没有指定 `ServerName` 时，服务器会尝试对 `IP` 地址进行反向查询来推断主机名。如果在 `ServerName` 中没有指定端口号，服务器会使用接受请求的那个端口。为了加强可靠性和可预测性，应该使用 `ServerName` 显式地指定一个主机名和端口号。

160 网管员必读——网络应用（第2版）

如果使用的是基于域名的虚拟主机，在<VirtualHost>段中的 ServerName 将是为了匹配这个虚拟主机，在“Host:”请求头中必须出现的主机名。

42. ServerPath 指令

该指令可以为兼容性不好的浏览器访问基于域名的虚拟主机保留 URL 路径名。其语法格式为：ServerPath URL-path。其作用域为：virtual host。

ServerPath 指令为主机设置了保守的（legacy）URL 路径名，与基于域名的虚拟主机配合使用。

43. ServerAdministrators 指令

该指令用于设置安装服务器的基础目录。其语法格式为：ServerAdministrators directory-path。其作用域为：server config，默认值为：ServerAdministrators /usr/local/apache。

ServerAdministrators 指令设置了服务器所在的目录。一般来说它将包含 conf/和 logs/子目录。其他配置文件的相对路径即基于此目录（比如 Include 或 LoadModule）。

例如：

```
ServerAdministrators /home/httpd
```

44. ServerSignature 指令

该指令用于配置服务器生成界面的页脚。其语法格式为：ServerSignature On|Off|EMail。其作用域为：server config、virtual host、directory 和.htaccess，默认值为：ServerSignature Off。

ServerSignature 指令允许配置服务器端生成文档的页脚（错误信息、mod_proxy 的 ftp 目录列表、mod_info 的输出）。启用这个页脚的原因主要在于处于一个代理服务器链中的时候，用户基本无法辨识出究竟是链中的哪个服务器真正产生了返回的错误信息。

默认的 Off 设置没有错误行（这样便与 Apache 1.2 及更旧版本兼容）。采用 On 会简单地增加一行关于服务器版本和正在伺服的虚拟主机的 ServerName，而 EMail 设置会如文档中说明的那样额外创建一个指向 ServerAdmin 的“mailto:”部分。

对于 2.0.44 以后的版本，显示的详细服务器版本号将由下面将要介绍的 ServerTokens 指令控制。

45. ServerTokens 指令

该指令用于配置“Server:”应答头。其语法格式为：ServerTokens Major|Minor|Min[imal]|Prod[uctOnly]|OS|Full。其作用域为：server config，默认值为：ServerTokens Full。

这个指令控制了服务器回应给客户端的“Server:”应答头是否包含关于服务器操作系统类型和编译模块的描述信息。

46. TimeOut 指令

该指令用于设置服务器在断定请求失败前等待的秒数。其语法格式为：TimeOut seconds。其作用域仅为：server config，默认值为：TimeOut 300。

TimeOut 指令用于设置 Apache 等待如下三种事件的时间长度。

- 接受一个 GET 请求耗费的总时间。
- POST 或 PUT 请求时，接受两个 TCP 包之间的时间。
- 应答时 TCP 包传输中两个 ACK 包之间的时间。

计时器在 1.2 版本之前的默认值为 1 200，而现在已经设置为 300 了，但对于绝大多数情况来说仍是足够的。没有把它默认值设得更小的原因在于代码里还有点问题：有时发送一个包之后，计时器没有复位。

47. <VirtualHost>指令

此指令设置包含仅作用于指定主机名或 IP 地址的指令。其语法格式为：<VirtualHost addr[:port] [addr[:port]] ...> ... </VirtualHost>。其作用域为：server config。

<VirtualHost>和</VirtualHost>用于封装一组仅作用于特定虚拟主机的指令。任何在虚拟主机配置中可以使用的指令也同样可以在这里使用。当服务器接受了一个特定虚拟主机的文档请求时，它会使用封装在<VirtualHost>配置段中的指令。Addr 可以是如下内容。

- 虚拟主机的 IP 地址。
- 虚拟主机 IP 地址对应的完整域名。

字符“*”仅与“NameVirtualHost *”配合使用，以匹配所有的 IP 地址；字符串“_default_”与基于 IP 的虚拟主机一起使用以捕获所有没有匹配的 IP 地址。

例如：

```
<VirtualHost 10.1.2.3>
ServerAdmin webmaster@host.foo.com
DocumentAdministrators /www/docs/host.foo.com
ServerName host.foo.com
ErrorLog logs/host.foo.com-error_log
TransferLog logs/host.foo.com-access_log
</VirtualHost>
```

每个虚拟主机必须对应不同的 IP 地址、端口号或是不同的主机名。在第一种情况下，服务器所在的物理机器必须配置为可以为多个 IP 地址接受 IP 包（在机器没有多个网络硬件界面的情况下，如果操作系统支持，可以使用 ifconfig alias 命令来达到这个目的）。



<VirtualHost>的使用并不影响 Apache 的监听地址。需要使用 Listen 来确保 Apache 正在监听正确的地址。

当使用基于 IP 的虚拟主机时，特殊的名称“_default_”可以在没有匹配到其他列出的虚拟主机的情况下，作为匹配任何 IP 地址的默认虚拟主机。在没有进行“_default_”虚拟主机的设定时，在没有 IP 与请求匹配的情况下，将使用“主服务器”（在所有虚拟主机配置段之外）的配置。但请注意：任何匹配 NameVirtualHost 指令的 IP 地址既不会使用“主服务器”配置，也不会使用“_default_”虚拟主机的配置。

用户可以指定一个“:port”来改变匹配的端口，如果没有指定，它将沿用主服务器中离它最近的那个 Listen 指定的值，也可以指定“:*”来匹配那个地址上的所有端口（使用“_default_”时，这是推荐采用的方法）。

3.2.6 Apache 服务器配置基本思路

理解了 Apache 的基本组成和指令后，接下来就可以正式配置我们的 Apache Web 服务器

162 网管员必读——网络应用（第2版）

了。但在正式进行配置之前，建议也像笔者一样，先理清一下整个服务器程序的配置思路，这样，配置起来的服务器系统就会更加严谨，思路更加清晰。

Apache 服务器的配置方法不再是图形界面方式，而基本上是在一个名为 `httpd.conf` 的进程配置文件中进行的，它是一个纯文本文件。相对于 Windows 界面的应用服务器配置来说，全文本配置文件配置方式的 Apache 服务器的配置显得要复杂许多，就像我们有许多读者朋友使用 UNIX 和 Linux 系统感觉非常困难、非常不方便一样。其实从安全性和性能方面来说，纯文本配置文件的配置更加安全、性能更加强劲。

安装 Apache 程序下面是配置 Apache 服务器的基本思路。

（1）安装 Apache 程序

这时的程序安装相对来说要简单许多，与服务器配置有关的配置项仅一个地方。具体安装过程将在本章的 3.3 节介绍，当然在这节中不会对详细的安装过程进行介绍，只对与服务器配置关系密切的方面进行介绍。另外，还将介绍服务器的初始调试。

具体将在本章 3.3 节介绍。

（2）Apache 服务器的全局配置

服务器程序安装并调试好后，接下来要对我们的 Apache Web 服务器进行全局配置。其中包括 Web 服务器标识、文件定位、资源使用限制等方面的配置。通过这些全局配置，一台基本的 Web 服务器就可以运行了。

安装 Apache 程序具体配置方法将在本章 3.4 节介绍。

Apache 服务器其他高级配置，因篇幅原因，本书就不再介绍了。

3.3 Apache 服务器程序的安装与调试

Apache 服务器程序的安装需要有 Microsoft Installer 1.2 或更高版本。Windows XP/2003 不需要升级即可安装。



使用这个安装包不能在同一台机器上安装两套同一版本的 Apache 系统。但是，在同一台机器上，安装一个 1.3 和一个 2.0 或 2.2 版本的 Apache 则没有问题。

1. Apache 程序的安装

运行已下载的上述 Apache .msi 文件。在程序安装过程中会要求提供以下信息（参见如图 3-4 所示的对话框）。

- Network Domain (网络域名): 你的服务器已经或者将要注册 DNS 域名 (不是全称)。比如，笔者所申请的一个免费的域名为 `lycbgz.xicp.net`，则这里所填写的 DNS 域名就为 `xicp.net`。
- Server Name (服务器主机名): 这是指服务器的全称 DNS 域名，也就是所申请的域名，如笔者所申请的域名，此处就应当在这里输入: `lycbgz.xicp.net`。
- Administrator's Email Address (管理电子邮件地址): 此处填上 Web 服务器管理员的 E-mail 地址。这个地址将会在默认的出错界面上显示给客户端。
- Install Apache HTTP Server 2.2 programs and shortcuts for: 如果你希望 Apache 在 80

端口监听，并被安装为服务（即使无人登录，Apache 仍将运行），就选择“for All Users, on Port 80, as a Service – Recommended”单选项；如果你希望将 Apache 安装为个人试验使用，或者已经有一个运行于 80 端口的 WWW 服务器，就选择“only for the Current User, on Port 8080, when started Manually”单选项。

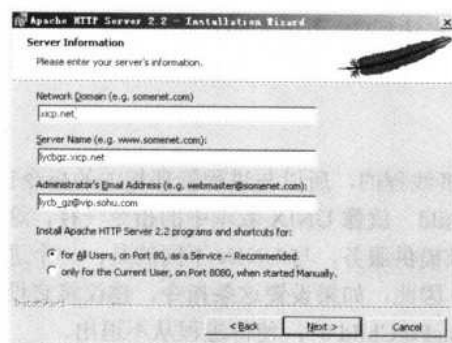


图 3-4 “Server Information”对话框

在安装期间，Apache 将会配置所选择的安装目录下的 conf 文件夹中的文件。但是如果那个目录下已有同名文件存在，原有文件将不会被覆盖，而相应的新文件将会被加上.default 扩展名。也就是说，如果 conf/httpd.conf 这个文件已经存在，那么不会对它作任何改变，而新版本 conf/httpd.conf 的内容将会被写入文件 conf/httpd.conf.default。安装完成以后你应该检查.default 文件中的内容看看有没有不同，建议你删除原来的那个 httpd.conf 文件，同时把新的 httpd.conf.default 文件改名为 httpd.conf。

而且，如果你以前已安装了一个 Apache 系统，则会在 htdocs 目录下有一个 index.html 主页文件，新安装的 Apache 不会被覆盖掉（也不会安装 index.html.default 文件）。这意味着在一个旧版本 Apache 上安装新版本是安全的，但必须在安装之前首先停掉原有服务器，然后在安装完成后重新启动它。启动正常时会在系统状态栏有一个带有绿色箭头的图标，双击即可打开如图 3-5 所示的对话框。在其中即可启动和停止 Apache 2.2 服务。

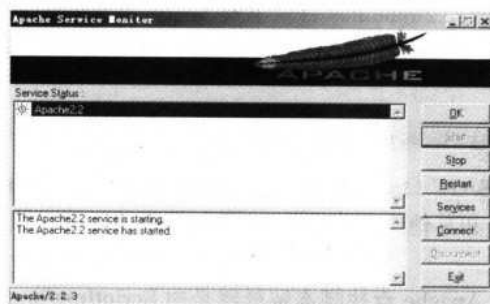


图 3-5 “Apache Service Monitor”控制台窗口

安装 Apache 以后，用户应该编辑 conf 目录下的配置文件。这些文件已在安装期间被配置好，以便 Apache 能够从安装目录运行，网站文件主目录被配置为安装目录下的子目录 htdocs。在开始真正使用之前，还有很多选项需要设置。但是为了尽快开始，可以使用安装

164 网管员必读——网络应用（第2版）

时自动配置的配置文件。

2. Windows 版本 Apache 的主要不同

Apache for Windows 相对 UNIX/Linux 版本来说，主要的不同之处有如下几点。

1) 线程方式不同

Apache for Windows 是多线程的，不像 UNIX 版本那样为每个请求使用一个单独的进程。这两个 Apache 进程包括：一个父进程和一个处理请求的子进程。在子进程内部由多个单独的线程来处理每个请求。

2) 指令不同

因为 Windows 版本是多线程的，所以与进程管理相关的指令也是不同的，主要包括：

- **MaxRequestsPerChild** 就像 UNIX 版本中的指令一样，这条指令控制一个进程退出前将为多少个请求提供服务。与 UNIX 不同的是，一个进程将为所有请求而不是只为一个请求服务。因此，如果设置这条指令，建议将它设为一个很大的值。默认设置为“MaxRequestsPerChild 0”，使得进程从不退出。



注意

启动新的子进程时将会重新读入服务器配置文件。如果修改了 httpd.conf，新的子进程将有可能不能启动或者可能得到预期之外的结果。

- **ThreadsPerChild** 这是一条新的指令，用来告诉服务器应该使用多少个线程，指明了服务器可以立刻处理的最大连接数。如果站点有大量的点击，请确认设置了足够大的值。推荐的默认设置是“ThreadsPerChild 50”。

3) 接收文件名不同

接收文件名作为参数的指令必须使用 Windows 文件名，而不是 UNIX 文件名。但是，因为 Apache 内部使用 UNIX 风格的名字，必须使用正斜杠 (/) 而不是反斜杠 (\)，也可以使用盘符；如果省略盘符，将假定使用 Apache 可执行文件所在的盘符。

4) 具有装入模块的能力

Apache for Windows 具有运行时装入模块的能力，不需要重新编译。如果 Apache 在正常情况下编译，它会在 \Apache2.2\modules 目录下安装许多可选模块。要激活它们或其他模块，必须使用新的 LoadModule 指令。如要激活状态模块，可使用下列指令（除了 access.conf 中的状态激活指令以外）。

```
LoadModule status_module modules/mod_status.so
```

Apache 也可以加载 ISAPI (Internet Server Applications Programming Interface) 扩展，例如被 Microsoft IIS 服务器和其他一些 Windows 服务器所使用的。但 Apache 不能加载 ISAPI 过滤器。

当运行 CGI 脚本时，Apache 查找脚本解释器是由 ScriptInterpreterSource 指令配置的。

5) 使用 .htaccess 类文件较困难

由于在 Windows 下管理具有像 .htaccess 这样名字的文件是很困难的，你会发现在配置文件中 使用 AccessFileName 指令改变它的文件名是很有用的。

6) 日志记录机制不同

在 Windows NT 上，Apache 启动时发生的错误将会记入 Windows 事件日志 (event log)。这个机制将在 Apache 尚不能使用 error.log 文件的时候运作。你可以通过“事件查看器”的 MMC 接口查看 Windows 事件日志。但要注意，在 Windows 9x 系统上不存在事件日志机制，因此，无法记录启动错误。

3. Apache 服务的启动与停止

如果配置文件中 Listen 定义的是默认的 80 端口（或 1024 以下），那么启动 Apache 将需要 Administrators 权限以将它绑定在特权端口上。一旦服务器开始启动并完成了一些诸如打开日志文件之类的准备操作，它将创建很多子进程来完成一些诸如侦听和回应客户端请求的工作。httpd 主进程仍然以 Administrators 用户的权限运行，而它的子进程将以一个较低权限的用户运行。这将由你选择的多路处理模块进行控制。

调用 httpd 可执行文件的推荐方法是使用 apachectl 控制脚本。此脚本设置了在某些操作系统中正常运行 httpd 所必需的环境变量，然后调用 httpd 二进制文件。apachectl 会传递命令行的所有参数，因此所有用于 httpd 的选项多半也可以用于 apachectl。你可以直接修改 apachectl 脚本，改变首部的 HTTPD 变量使之指向 httpd 可执行文件的正确位置，也可以设置任意的命令行参数，使之总是有效。

httpd 被调用后第一件要做的事情就是找到并读取配置文件 httpd.conf。此文件的位置是在编译时设定的，但也可以像下面这样在运行时用 -f 选项来指定：

```
/program files/apache software foundation/apache2.2/bin/apachectl -f /program files/apache software foundation/apache2.2/conf/httpd.conf
```

如果启动过程一切正常，服务器将与终端分离并几乎立即出现命令行提示符。这表示服务器已经启动并开始运行。然后你就可以用你的浏览器去连接你的服务器来查看 DocumentAdministrators 目录下的测试文档及其界面链接里的其他文档的本地副本。

如果 Apache 在启动过程中发生了致命错误，它将在退出前把描述这个错误的信息显示在终端上或者写入到 ErrorLog 中。一个最常产生的错误信息是“Unable to bind to Port ...”，这主要由以下原因造成。

- 想由一个特权端口启动服务但没有以 Administrators 用户运行。
- 启动服务时已经有另外的 Apache 实例在运行，或其他 web 服务器已经绑定了同样的端口。

如果希望服务器在系统重启后仍保持运行状态，应该把 apachectl 的调用加入到系统的启动文件中（通常为 rc.local 文件或 rc.N 目录下的某一文件）。这将会以 Administrators 权限启动 Apache。当然，在此之前，必须保证服务器已经完成了安全和访问权限的设定。

apachectl 脚本被设计为可以用做 SysV 初始化脚本，它接受 start、restart、stop 参数，并把它们翻译为 httpd 对应的信号，所以通常都可以将 apachectl 连接到适当的初始目录，但是需要检查系统对此的精确要求。

Apache 仅能够在 Windows NT 上作为服务运行。

用户可以选择在安装 Apache 时自动将其安装为一个服务。如果选择“for All Users”单选项（参见图 3-4），那么 Apache 将会被安装为服务。如果选择了“only for the Current User”

166 网管员必读——网络应用（第2版）

单选项（参见图 3-4），可以在安装后手动将 Apache 注册为服务。需要注意的是，必须是 Administrators 组的成员才能成功注册服务。

使用 Apache Service Monitor 工具（参见图 3-5），可以查看和管理所在网络上的所有机器上安装的 Apache 服务的状态。为了能够使用这个工具管理 Apache 服务，就必须首先自动或手动安装 Apache 服务。

用户可以在 Apache 安装目录的 bin 子目录下，使用如下命令将 Apache 安装为 Windows NT 服务：apache -k install。

当在同一机器上安装多个 Apache 服务时，就必须为它们指定不同的名字。如果想指定服务的名称，那么可以使用命令：

```
apache -k install -n “服务名”
```

如果想为不同名称的服务使用不同的配置文件，则安装后需要指定配置文件，执行命令如：apache -k install -n “服务名” -f “c:\files\my.conf”（示例，根据实际更改配置文件的位置和配置文件名）。

如果使用的是 apache -k install -n 命令，则除 -k install 外没有其他命令行参数，那么被安装的服务名称将是：Apache 2.2，配置文件将使用 conf\httpd.conf。

要移除一个 Apache 服务很简单，只需在 bin 子目录下执行：apache -k uninstall。或者使用下述命令移除特定名称的 Apache 服务：

```
apache -k uninstall -n “服务名”
```

通常，启动、重启、关闭 Apache 服务可在 Apache Service Monitor 工具窗口（参见图 3-5）中进行。另外也可以使用控制台命令：NET START Apache 2.2 和 NET STOP Apache 2.2，或者通过 Windows “服务”窗口，如图 3-6 所示。在启动 Apache 服务之前，应当使用下面的命令检查一下配置文件的正确性：

```
apache -n “服务名” -t。
```



图 3-6 “服务”窗口中的“Apache 2.2”服务

用户可以通过命令行开关来控制 Apache 服务。要启动一个已经安装的 Apache 服务，可以使用：apache -k start。要停止一个已经安装的 Apache 服务，可以使用：apache -k stop 或：

apache -k shutdown。要重启一个运行中的 Apache 服务，强制它重新读取配置文件，可以使用：apache -k restart。

4. 运行 Apache 服务的账户

在默认情况下，Apache 服务将被注册为以本地系统用户（LocalSystem 账号）身份运行。LocalSystem 账号没有网络权限，不能通过任何 Windows 安全机制访问网络，包括文件系统、命名管道、DCOM 或 secure RPC，但是它对于本地资源却拥有广泛的特权。

注意 永远不要把网络权限授予 LocalSystem 账号，如果需要 Apache 能够访问网络资源，最好按照下述方法为 Apache 另外建立一个单独的账号。用户应该建立一个单独的账号来运行 Apache 服务。特别是在必须通过 Apache 访问网络资源的时候。

以下是为运行 Apache 服务创建账号的步骤。

- (1) 创建一个普通域用户账号。
- (2) 授予这个新建的账号作为服务登录和作为操作系统一部分运行权限。在 Windows 2000/XP/2003 上可以使用组策略，或通过“本地安全策略”控制台来完成这个操作，只需在“以操作系统方式操作”和“作为服务登录”权利选项中添加相应用户账号即可，如图 3-7 所示。



图 3-7 在组策略中配置 Apache 服务账户所对应的两个选项

- (3) 确认新建的账号是 Users 组的一个成员。
 - (4) 确认新建的账号具有读取和执行所有文档和脚本目录（例如，Aapche 服务器程序安装目录下的 htdocs 和 cgi-bin 子目录）的权限。
 - (5) 确认新建的账号对 Apache 的 logs 目录具有读/写/删除（RWD）的权限。
 - (6) 确认新建的账号对 Apache.exe 二进制文件具有读取和执行（RX）的权限。
- 最好赋予运行 Apache 服务的用户读取和执行（RX）整个 Apache 2.2 目录的权限，并且对 logs 子目录具有读/写/删除（RWD）的权限。

如果允许使用这个账号作为一个用户和服务登录，就可以用这个账号登录上去测试执行脚本、读取 Web 页的权限，还可以通过控制台窗口启动 Apache。如果这样工作正常，又执行了上述的操作，那么 Apache 就能够正常地作为服务运行了。

5. 程序安装后的测试

启动 Apache 运行以后（不管是控制台窗口还是作为服务），它会在 80 端口上进行监听（除非改变了配置文件中的 Listen 指令）。要连接到服务器访问默认界面，启动一个浏览器

并输入下列 URL：

```
http://localhost/
```


在 2.0 版本及以前，在以上主页中会出现一个欢迎界面，并且界面上有到 Apache 用户手册的链接，而在 2.2 版本中仅显示 “It works”，如图 3-8 所示，表明 Aapache 服务器工作正常。如果什么都没有发生或是得到了一个错误，检查 logs 子文件夹中的 error.log 文件。如果主机没有联网或者 DNS 配置有严重问题，那么就需要输入这样的 URL：http://127.0.0.1/。




图 3-8 Apache 安装后默认的网站主页

如果将 Apache 配置为在非 80 端口监听（比如 8080），那么就应当使用下面的 URL 明确指定端口：http://127.0.0.1:8080/。当然，在实际应用中，我们需要把自己的网站文件放到 apache2.2/htdocs 网站文件目录中，并把主页文件名改为 index.html。

一旦基本配置可以工作了，就应该编辑 conf 目录下的文件来恰当地配置 Apache。此外，如果改变了作为 NT 服务运行的 Apache 的配置，就应该首先尝试从命令行启动来保证能够正确地启动 Apache 服务。

**注意**

因为 Apache 不能与其他 TCP/IP 应用程序（如 IIS）共享同一端口，你可能需要先停止、卸载或者重新配置某些特定的服务。这包括（但不限于）其他的 Web 服务器和 BlackIce 那样的防火墙。如果只能在禁止其他服务的情况下启动 Apache，那么需要重新配置 Apache 或者其他程序使它们不监听同一个 TCP/IP 端口。

**说明**

在 Apache 中默认的网站主页文件名就是 index.html，而不能是其他名称。如果把网站主页文件名改为其他的，就不会正确显示网站主页，而是列表显示网站的所有文件，由用户自己来选择主页文件，如图 3-9 所示。当然也可以通过 DirectoryIndex 指令更改，具体将在本章后面介绍。



图 3-9 更改主页文件名后进入网站的界面显示

3.4 Apache 服务器的全局配置

Apache HTTP Server 的配置与平常我们所见的 Windows 程序配置方法不一样，它不是采用图形界面方式，而是直接编辑其中的专用配置文件。自 2.0 版本以后，就把以前版本中的 3 个配置文件（httpd.conf、srm.conf 和 access.conf）放在了一起，集中在 httpd.conf 配置文件中。这个配置文件存放在 \Apache Software Foundation\Apache2.2\conf 目录下（参见图 3-2）。Apache 服务器可以不加任何配置改动，运行安装时默认配置的 Apache 服务器即可成功运行。但如果需要调整 Apache 服务器的性能，以及增加对某种特性的支持，就需要具体配置了。

用鼠标左键双击 httpd.default 主配置文件，可以看到其中包括许多配置选项，如图 3-10 所示。配置文件中的 # 表示行为配置选项的说明，或者指令注释。

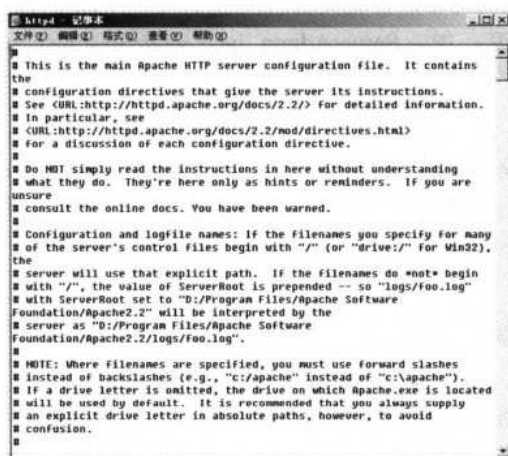


图 3-10 httpd.default 配置文件

在整个服务器全局配置中，主要涉及到：服务器标识、文件定位和资源使用限制三个方面。下面分别予以介绍。不过，因为主要指令在本章前面已做了介绍，所以在此仅对指令在配置方面进行简要说明。

3.4.1 服务器标识配置

在服务器标识方面，主要涉及到的指令包括：ServerName、ServerAdmin、ServerSignature、ServerTokens、UseCanonicalName 和 UseCanonicalPhysicalPort。

ServerAdmin 和 ServerTokens 指令控制有关服务器的哪些信息将出现在服务器生成的文档中（如错误消息）。ServerTokens 指令设置服务器 HTTP 响应头字段的值。

ServerName、UseCanonicalName 和 UseCanonicalPhysicalPort 指令用来决定怎样构建自引用 URL。如某客户端对一个目录发出请求，但没有包含目录名最后的斜线“/”，Apache 将重定向到客户端到包含“/”的全名，以使得客户端可以正确解析文档中的相对引用。

170 网管员必读——网络应用（第2版）

1. ServerName

配置服务器名称（域名）和端口。这个服务器名称就是站点名称（或称网址），如笔者目前所配置的 `lycbgz.xicp.net`，因为要在互联网上使用，这个域名需先向有关机构申请注册。同时在此处还将配置此站点 HTTP 协议所使用的端口。配置格式为：“ServerName 名称：端口”，如 `lycbgz.xicp.net:80`。



不一定是 80 号端口，因为端口号也是服务器的一种标识，这在介绍 IIS 网站时已有说明。但如果改用其他端口，则用户在访问时一定要加上端口号，如改为 8080，则需在浏览器中输入 `lycbgz.xicp.net:8080`。

2. ServerAdmin

配置服务器管理员邮箱。这个邮箱将在用户访问个人站点服务器时出错，在系统返回浏览器时给出，以便用户及时与站点管理员联系。当然，这个邮箱应该是有效的。配置格式为：ServerAdmin 管理员邮箱。如，ServerAdmin `lycb_gz@vip.sohu.com`，则配置管理邮箱为 `lycb_gz@vip.sohu.com`。

3. ServerSignature

该指令允许配置服务器端生成文档的页脚（错误信息、`mod_proxy` 的 `ftp` 目录列表、`mod_info` 的输出）。启用这个页脚的原因主要在于处于一个代理服务器链中的时候，用户基本无法辨识出究竟是链中的哪个服务器真正产生了返回的错误信息。

其语法格式为：

```
ServerSignature On|Off|Email
```

其默认值为“Off”，设置没有错误行（这样便与 Apache 1.2 及更旧版本兼容）。采用“On”设置会简单地增加一行关于服务器版本和正在伺服的虚拟主机的 ServerName，而“Email”设置会如文档中说明的那样额外创建一个指向 ServerAdmin 的“mailto:”部分。对于 2.0.44 以后的版本，显示的详细服务器版本号将由下面将要介绍的 ServerTokens 指令控制。

4. ServerTokens

这个指令控制了服务器回应给客户端的“Server:”应答头是否包含关于服务器操作系统类型和编译模块的描述信息。

其语法格式为：

```
ServerTokens Major|Minor|Min[imal]|Prod[uctOnly]|OS|Full
```

此设置将作用于整个服务器，而且不能用在虚拟主机的配置段中。2.0.44 版本以后，这个指令还控制着 ServerSignature 指令的显示内容。

5. UseCanonicalName

其语法格式为：

```
UseCanonicalName On|Off|DNS
```

在很多情况下，Apache 必须构造一个自引用 URL（一个指回相同服务器的 URL）。使用 UseCanonicalName 的“On”设置会将 ServerName 这个域名用于所有自引用 URL、

SERVER_NAME、CGI 中的 SERVER_PORT。

设置为 UseCanonicalName Off 时，如果客户端提供了主机名和端口（否则将如上所述使用标准域名），Apache 将会使用这些信息来构建自引用 URL。这些值与用于实现基于域名的虚拟主机的值相同，并且对于同样的客户端可用。CGI 变量 SERVER_NAME 和 SERVER_PORT 也会由客户端提供的值来构建。

“DNS”是为大量基于 IP 的虚拟主机支持那些不提供“Host:”应答头的浏览器使用的。使用这个选项时，Apache 将对客户端连入的服务器的 IP 地址进行反向 DNS 查询，以构建自引用 URL。

6. UseCanonicalPhysicalPort

这个指令与 UseCanonicalName 是配合使用的。其基本语法格式为：UseCanonicalPhysicalPort On|Off，默认值为：“Off”。

在 UseCanonicalPhysicalPort 指令中取值“On”时，Apache 将有可能在构造服务器的规范端口时，为了符合 UseCanonicalName 指令而使用实际的物理端口号（physical port）。在取值“Off”的时候，Apache 将不会使用实际的物理端口号，而是依赖所有已经配置的信息来构造一个合法的端口号。

决定使用物理端口号的次序如下：

当 UseCanonicalName 指令取值为“On”时的顺序如下。

- (1) ServerName 指定的端口号。
- (2) 物理端口号。
- (3) 默认端口号。

当 UseCanonicalName 指令取值“Off”或者“DNS”时的顺序如下。

- (1) “Host:”请求头提供的端口号。
- (2) 物理端口号。
- (3) Servername 指定的端口号。
- (4) 默认端口号。

3.4.2 文件定位配置

“文件定位”就是指网站文件的定位，如 Apache 程序内核存储目录、网站主目录位置、日志文件位置、锁定的文件位置等。相关指令包括：CoreDumpDirectory、DocumentAdministrators、ErrorLog、LockFile、PidFile、ScoreBoardFile 和 ServerAdministrators。

这些指令控制 Apache 正常工作所需的各种文件的定位。如果路径名不以斜杠 (/) 开头，那么就认为该文件是相对于 ServerAdministrators 指令所定义的相对路径，需要注意路径中的文件哪些对非 Administrators 用户来说是可写的。

1. CoreDumpDirectory

这个指令用于控制 Apache 程序使用的内核存储目录。默认位于 ServerAdministrators 指令配置的路径下。这个目录通常对于运行服务器的用户是不可写的，内核存储一般也就不会写入内容。如果在调试中需要内核存储，那么就可以用这个指令来指定另外一个目录。其语法格式为：CoreDumpDirectory directory。

172 网管员必读——网络应用（第2版）

2. DocumentAdministrators

此指令设置了 httpd 进程所服务的网站主目录。在没有使用类似 Alias 这样的指令的情况下，服务器会将请求中的 URL 附加到 DocumentAdministrators 指令所指定的路径后面，以构成指向文档的路径。其语法格式为：DocumentAdministrators directory-path。默认值为：/apache2.2/htdocs。我们也可以自定义网站主目录，例如：

```
DocumentAdministrators /usr/web
```

这样一来，用户网站的访问会直接指向 /usr/web/index.html。如果 directory-path 不是绝对路径，则被假定为是相对于 ServerAdministrators 指令指定的路径。需要注意的是，指定 DocumentAdministrators 时不应包括最后的“/”。

3. ErrorLog

ErrorLog 指令指定了当服务器遇到错误时记录错误日志的文件。其语法格式为：ErrorLog file-path[syslog[:facility]]，默认值为：logs 子目录下的 error.log 文件。如果 file-path 不是一个以斜杠 (/) 开头的绝对路径，那么也将被认为是一个相对于 ServerAdministrators 指令指定的相对路径。例如：

```
ErrorLog /var/log/httpd/error_log
```

如果 file-path 以一个管道符号 (|) 开头，那么会为它指定一个命令来处理错误日志。例如：

```
ErrorLog "|/program files/apache software foundation/apache2.2/bin/httpd_errors"
```

4. LockFile

LockFile 指令设置当 AcceptMutex 指令的值是 fcntl 或 flock 的时候，Apache 使用的锁文件的位置。其语法格式为：LockFile filename，默认值为 logs 子目录下的 accept.lock 文件。该指令通常保持它的默认值。改变默认值的主要原因是 logs 目录位于一个 NFS 文件系统上，因为锁文件必须位于本地磁盘上。主服务器进程的 PID 会自动添加到文件名后面。



最好不要将此文件放在任何人都可以具有写权限的目录（比如 /var/tmp）中，因为其他人可以通过建立一个与服务器企图建立的锁文件同名的文件，来阻止服务器启动，从而造成一个拒绝服务的攻击。

5. PidFile

PidFile 指令设置服务器用于记录父进程（监控进程）PID 的文件。如果指定的不是绝对路径，那么将视为基于 ServerAdministrators 指令指定的相对路径。其语法格式为：PidFile filename，默认值为：logs 子目录下的 httpd.pid 文件。例如：

```
PidFile /var/run/apache.pid
```

这个文件通常用来为服务器父进程发送一个信号，用于关闭或重启服务器，以重新打开 ErrorLog 和 TransferLog 文件，重新读取配置文件。这些可以通过发送一个“SIGHUP”（kill -1）信号到 PidFile 记录的进程 PID。

PidFile 和其他日志文件一样要注意放置位置和安全问题。需要注意的是，从 Apache 2 版本开始，推荐使用 apachectl 脚本来启动或停止服务器。

6. ScoreBoardFile

ScoreBoardFile 指令存储子进程协调数据（coordination data）的文件。其语法格式为：ScoreBoardFile file-path，默认值为：logs 子目录下的 apache_status 文件。

Apache 使用记分板（scoreboard）在父进程和子进程之间进行通信。一些体系结构要求有一个文件来帮助通信。如果未指定这个文件，Apache 会首先尝试在匿名共享内存中建立完整的记分板（scoreboard），若失败，将继续尝试使用基于文件的共享存储器在磁盘上建立这个文件。若利用这个指令指定这个文件的位置，则 Apache 将总是在磁盘上建立这个文件。例如：

```
ScoreBoardFile /var/run/apache_status
```

基于文件的共享存储器对于使用直接访问记分板（scoreboard）的第三程序是很有用的。将 ScoreBoardFile 放置在 RAM disk 中会对速度提升有很大帮助。但是同其他日志文件一样也要注意放置位置和安全问题。

7. ServerAdministrators

ServerAdministrators 指令设置了服务器所在的目录。一般来说它将包含 conf/和 logs/两个子目录。其他配置文件的相对路径即基于此目录（比如 Include 或 LoadModule）。其语法格式为：ServerAdministrators directory-path，默认值为：/program files/apache software foundation/apache2.2。也可以自定义这个目录，这样就改变了其他相对路径的相对位置，例如：

```
ServerAdministrators /home/httpd
```

3.4.3 资源使用限制配置

“资源使用限制”就是要限制用户对网站特定资源（如目录、服务器硬件等）的访问。相关指令包括：LimitRequestBody、LimitRequestFields、LimitRequestFieldSize、LimitRequestLine、RLimitCPU、RLimitMEM、RLimitNPROC 和 ThreadStackSize。

LimitRequest*系列指令用来限制 Apache 在读取客户端请求的过程中使用的资源数量。通过限制这些值，可以减轻某些拒绝服务（DOS）攻击；RLimit*系列指令限制被 Apache 子进程所派生的进程使用的资源数量，通常这些指令用来控制 CGI 脚本和 SSI exec 命令所使用的资源；ThreadStackSize 指令在某些平台上用来控制堆栈大小。

1. LimitRequestBody

LimitRequestBody 指令限制客户端发送的 HTTP 请求体的最大字节长度。其语法格式为：LimitRequestBody Bytes，Bytes 在 0（意味着无限制）到 2 147 483 647（2GB）间限制了请求体所允许的字节数。默认值为“0”。

LimitRequestBody 指令可以让用户在其作用范围内（整个服务器、特定目录、特定文件、特定位置）设置一个允许客户端发送的 HTTP 请求体的最大字节长度的限制。如果客户端的请求超出了这个限制，服务器会回应一个错误，而不是为这个请求继续提供服务。一个普通请求的信息在很大程度上取决于资源的自然属性和这个资源允许的方法。CGI 脚本经常用消息体把表单的信息传递给服务器。使用 PUT 方法至少能够得到与服务器期望从这个资源得到的信息量差不多大小的值。

174 网管员必读——网络应用（第2版）

此指令给了服务器管理员更大的可控性，以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。比如，如果允许文件上传到某个位置，而且希望能将上传文件的大小设置为 100KB，可以使用下面的指令：

LimitRequestBody 102400

2. LimitRequestFields

LimitRequestFields 用来限制接受客户端请求中 HTTP 请求头域的数量。其语法格式为：**LimitRequestFields Number**，**Number** 是一个 0（意味着不限）到 32 767 之间的整数。默认值为“100”。默认值为编译时的常量 **DEFAULT_LIMIT_REQUEST_FIELDS**（发布值为 100）。

LimitRequestFields 指令允许服务器管理员修改在一个 HTTP 请求中的请求头域的数量限制。服务器需要此值大于一个普通客户端请求中包含头域的数量。一个客户端请求头域的数量很少大于 20，但根据客户端的不同这个数字有很大的差别，经常取决于用户配置他们的浏览器扩展以支持更详细的内容协商。可选的 HTTP 扩展经常使用请求头域来实现。

这个指令给了服务器管理员更大的可控性，以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。如果正常使用的客户端得到了服务器的错误应答，指出其在请求中发送了过多的头域，你应该适当地增大此值。例如：

LimitRequestFields 50

3. LimitRequestFieldSize

LimitRequestFieldSize 指令用来限制客户端发送的请求头的字节数。其语法格式为：**LimitRequestFieldSize Bytes**，**Bytes** 指定了 HTTP 请求头允许的字节大小。默认值为“8190”。

LimitRequestFieldSize 指令允许服务器管理员增加，或减少 HTTP 请求头域大小的限制。一般来说，服务器需要此值足够大，以适应普通客户端的任何请求的头域大小。一个普通头域的大小对于不同的客户端来说是有很大差别的，一般与用户配置他们的浏览器以支持更多的内容协议密切相关。

这个指令给了服务器管理员更大的可控性，以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。例如：

LimitRequestFieldSize 4094

一般情况下，请不要改变这个设置，而是保持其默认设置。

4. LimitRequestLine

LimitRequestLine 指令用来限制接收客户端发送的 HTTP 请求行的字节数。其语法格式为：**LimitRequestLine Bytes**，**Bytes** 将设置 HTTP 请求行的字节数限制。默认值也为“8190”。

LimitRequestLine 指令允许服务器管理员增加或减少客户端 HTTP 请求行允许大小的限制。因为请求行包括 HTTP 方法、URI、协议版本，所以 **LimitRequestLine** 指令会限制请求 URI 的长度。服务器会需要这个值足够大以装载它所有的资源名，包括可能在 GET 请求中所传递的查询部分的所有信息。

这个指令也给了服务器管理员更大的可控性，以控制客户端不正常的请求行为。这有助于避免某些形式的拒绝服务攻击。例如：

LimitRequestLine 4094

一般情况下，不需要改变此设置的默认值。

5. RLimitCPU

RLimitCPU 指令用来限制 Apache 子进程派生的进程占用 CPU 的最大秒数。CPU 资源限制表示为每进程占用的秒数。其语法格式为：RLimitCPU seconds|max [seconds|max]，默认值未定义，使用操作系统默认值。

第一个参数设置了所有进程的软资源限制，第二个参数设置了最大资源限制。两个参数均可设置为一个数值，或是“max”，以表示设置为操作系统允许的最大值。增大此资源限制最大值需要以 root 运行服务器或是在初始化启动语句中进行设置。

这个限制将作用于 Apache 子进程服务的请求所衍生出来的进程，而不是 Apache 子进程本身。这个范围包括 CGI 脚本和 SSI 执行命令，但不包括所有从 Apache 父进程衍生出来的进程。比如，管道日志。

6. RLimitMEM

RLimitMEM 指令用来限制由 Apache 子进程派生的进程占用的最大内存字节数。内存资源限制表示为每进程占用的字节数。其语法格式为：RLimitMEM Bytes|max [Bytes|max]，也没有定义默认值，使用操作系统默认值。

第一个参数设置了所有进程的软资源限制，第二个参数设置了最大资源限制。两个参数均可设置为一个数值，或是“max”，以表示设置为操作系统允许的最大值。增大此资源限制最大值需要以 root 运行服务器或是在初始化启动语句中进行设置。

这个限制将作用于 Apache 子进程服务的请求所衍生出来的进程，而不是 Apache 子进程本身。这个范围包括 CGI 脚本和 SSI 执行命令，但不包括所有从 Apache 父进程衍生出来的进程。比如，管道日志。

7. RLimitNPROC

RLimitNPROC 指令用来限制由 Apache 子进程派生的进程所派生的进程数目。进程限制控制了每个用户的进程数。其语法格式为：RLimitNPROC number|max [number|max]，也没有定义默认值，使用操作系统默认值。

第一个参数设置了所有进程的软资源限制，第二个参数设置了最大资源限制。两个参数均可设置为一个数值，或是“max”，以表示设置为操作系统允许的最大值。增大此资源限制最大值需要以 administrator 账户运行服务器或是在初始化启动语句中进行设置。

这个限制将作用于 Apache 子进程服务的请求所衍生出来的进程，而不是 Apache 子进程本身。这个范围包括 CGI 脚本和 SSI 执行命令，但不包括所有从 Apache 父进程衍生出来的进程。比如，管道日志。



注意

如果 CGI 进程不是以 Web 服务器的 uid 启动的，那么这个指令将限制服务器自己能够创建的进程数目。此种情况将在 error_log 中以“cannot fork”进行记录。

8. ThreadStackSize

ThreadStackSize 指令用来处理客户端连接的线程使用的栈尺寸（字节）。其语法格式为：ThreadStackSize size，在 NetWare 系统中默认值为 65 536；其他系统中等于操作系统默认值。

176 网管员必读——网络应用（第2版）

`ThreadStackSize` 指令设置了处理客户端连接（包括调用模块以协助处理）的线程允许使用的最大栈尺寸（字节）。在大多数情况下，操作系统默认的栈尺寸很合理，但是在某些情况下，需要调整这个值。如，在默认栈尺寸较小的平台上（比如 HP-UX），Apache 可能会在使用一些需要较大栈尺寸的第三方模块时崩溃。这样的问题可以通过将 `ThreadStackSize` 设置为一个较大的值来解决。这种调整应当仅仅在第三方模块提供者明确要求的情况下才需要，或者是通过诊断确定是由于栈空间太小而导致崩溃。

而在某些平台上，如果默认的栈空间大于服务器运行所需空间，那么将 `ThreadStackSize` 值降低到小于操作系统默认值可以让每个进程中允许生成的最大线程数量增加。这种类型的调整应该仅在测试环境中使用，并且对所有服务器进程进行充分的测试，因为处理某些罕见的请求需要较大的栈空间。一个很小的服务器配置变化就有可能使得当前的 `ThreadStackSize` 设置变得不合适。

3.4.4 其他全局配置

除了以上介绍的服务器标识、文件位置和资源限制三个方面的全局配置外，在 Apache 服务器的 `httpd.conf` 的开始部分还有一些其他配置也是非常重要的，本节将分别予以介绍。

1. Timeout

设置连接请求的最大延时，超过这个设置，即自动断开，单位为秒。其语法格式为：`Timeout seconds`，默认值为：300，配置最大延时为 300 秒。`Timeout` 指令用于设置 Apache 等待如下 3 种事件的时间长度。

- 接受一个 GET 请求耗费的总时间。
- POST 或 PUT 请求时，接受两个 TCP 包之间的时间。
- 应答时 TCP 包传输两个 ACK 包之间的时间。

计时器在 1.2 版本之前的默认值为 1200，而现在已经设置为 300 了，但对于绝大多数情况来说仍是足够的。没有把默认值设得更小的原因在于代码里还有点问题：有时发送一个包之后，计时器没有复位。

2. KeepAlive

该指令设置是否允许永久进行 HTTP 连接。`Keep-Alive` 指令扩展自 HTTP/1.0 和 HTTP/1.1 的持久链接特性，其语法格式为：`KeepAlive On|Off`。提供了长效的 HTTP 会话，用于在同一个 TCP 连接中进行多次请求。在某些情况下，这样的方式会对包含大量图片的 HTML 文档造成的延时起到 50% 的加速作用。在 Apache 1.2 版本以后，可以设置 `KeepAlive On`，以启用持久链接，这也是默认设置。

对于 HTTP/1.0 的客户端来说，仅当客户端指定使用的时候才会使用持久链接连接。此外，仅当能够预先知道传输的内容长度时，才会与 HTTP/1.0 的客户端建立持久链接连接。这意味着那些长度不定的内容，诸如 CGI 输出、SSI 界面，以及服务器端生成的目录列表等内容一般来说将无法使用与 HTTP/1.0 客户端建立的持久链接连接。而对于 HTTP/1.1 的客户端来说，如果没有进行特殊指定，持久链接将是默认的连接方式。如果客户端进行了请求，将使用分块编码以解决在持久链接里发送未知长度内容的问题。

3. MaxKeepAliveRequests

MaxKeepAliveRequests 指令限制了当启用 KeepAlive 配置时，每个连接允许的请求数量。其语法格式为：MaxKeepAliveRequests number，默认值为：100，允许的最多请求数为 100 个。如果将此值设为“0”，将不限制请求的数目。我们建议最好将此值设为一个比较大的值，以确保最优的服务器性能。

4. Listen

Listen 指令指示 Apache 只在指定的 IP 地址和端口上监听。在默认情况下，Apache 会在所有 IP 地址上监听。其语法格式为：Listen [IP-address:]portnumber [protocol]。该指令在 Apache 2.0 以后版本中必须设置，protocol 参数仅在 2.1.5 及以后版本中可用。如果在配置文件中找不到这个指令，服务器将无法启动。这和以前的版本不一样。

Listen 指令指定服务器在那个端口或地址和端口的组合上监听接入请求。如果只指定一个端口，服务器将在所有地址上监听该端口。如果指定了地址和端口的组合，服务器将在指定地址的指定端口上监听。

使用多个 Listen 指令可以指定多个不同的监听端口或地址端口组合。服务器将会对列出的所有端口和地址端口组合上的请求做出应答。

设置服务器要绑定的端口、IP 地址，或者是两者的组合。以替代系统默认绑定值。如 Listen 12.35.56.78:80，绑定 IP 地址为 12.35.56.78，同时绑定这个地址中的 80 号端口；Listen 80 设定服务器绑定 80 号端口。在此需要与所申请的固定互联网 IP 地址进行绑定。



Apache 一般来说不需要进行绑定其他 IP 地址和端口设置，因为它会自动绑定在本机所有 IP 地址的 80 号端口上。

5. DirectoryIndex

DirectoryIndex 指令设置了当客户端在请求的目录名的末尾刻意添加一个“/”以表示请求该目录的索引时，服务器需要寻找的资源列表，也就是指定网站主页文件。其语法格式为：DirectoryIndex local-url [local-url] ... Local-url 是一个相对于被请求目录的文档的 URL（通常是那个目录中的一个文件）。可以指定多个 URL，服务器将返回最先找到的那一个。若一个也没有找到，并且那个目录设置了 Indexes 选项，服务器将会自动产生一个那个目录中的资源列表。默认值就是 index.html。

从语法格式中可以看出，它可以指定多个文件名，各文件之间要以空格分隔，而且还可以是不是位于同一目录下的文件。例如：

```
DirectoryIndex index.html index.txt /cgi-bin/index.pl
```

这些默认主页文件名也有优先级别差异，越靠前级别越高，越优先执行。

在 httpd.conf 配置的“Main server configuration”（主服务器配置）部分有如下几个指令需要配置：

6. Order

这是一个用于控制目录可访问状态的配置选项。它的配置格式为：Order ordering，默认值为：Deny 和 Allow。Ordering 取值范围是以下几种范例之一。

178 网管员必读——网络应用（第2版）

- **Deny,Allow** Deny 指令在 Allow 指令之前被评估。默认允许所有访问，任何不匹配 Deny 指令或者匹配 Allow 指令的客户都被允许访问。
- **Allow,Deny** Allow 指令在 Deny 指令之前被评估。默认拒绝所有访问，任何不匹配 Allow 指令或者匹配 Deny 指令的客户都将被禁止访问。
- **Mutual-failure** 只有出现在 Allow 列表并且不出现在 Deny 列表中的主机才被允许访问。这种顺序与“Order Allow,Deny”具有同样效果，不赞成使用。

关键字只能用逗号分隔；它们之间不能有空格。注意在所有情况下每个 Allow 和 Deny 指令语句都将被评估。

在下面的例子中，apache.org 域中所有主机都允许访问，而其他任何主机的访问都将被拒绝。

```
Order Deny,Allow
Deny from all
Allow from apache.org
```

在下面的例子中，apache.org 域中所有主机，除了 foo.apache.org 子域包含的主机被拒绝以外，其他都允许访问。而所有不在 apache.org 域中的主机都不允许访问，因为默认状态是拒绝对服务器的访问。

```
Order Allow,Deny
Allow from apache.org
Deny from foo.apache.org
```

另一方面，如果上个例子中的 Order 指令改变为“Deny,Allow”，将允许所有主机的访问。这是因为，不管配置文件中指令的实际顺序如何，“Allow from apache.org”指令会最后被评估并覆盖之前的“Deny from foo.apache.org”。所有不在 apache.org 域中的主机也允许访问是因为默认状态被改变到了允许。

即使没有伴随 Allow 和 Deny 指令，一个 Order 指令的存在也会影响服务器上某一个部分的访问，这是由于它对默认访问状态的影响。例如：

```
<Directory /www>
Order Allow,Deny
</Directory>
```

这样将会禁止所有对/www 目录的访问，因为默认状态将被设置为拒绝。

Order 指令只在服务器配置的每个段内部控制访问指令的处理。这暗示着，例如，一个在<Location>段中出现的 Allow 或 Deny 指令，总是会在一个<Directory>段或者.htaccess 文件中出现的 Allow 或 Deny 指令之后被评估，而不管 Order 指令如何设置。

7. Alias

Alias 指令使文档可以被存储在 DocumentRoot 以外的本地文件系统中。以 url-path 路径开头的 URL 可以被映射到以 directory-path 开头的本地文件。其语法格式为：RL-path file-path|directory-path，例如，Alias /image /ftp/pub/image。这样对“http://myserver/image/foo.gif”的请求，服务器将返回“/ftp/pub/image/foo.gif”文件。因为仅匹配完整路径，所以上述例子不会匹配对“http://myserver/image/foo.gif”的请求。

这个选项就相当于 IIS 和 PWS 等 Web 服务器软件中的虚拟目录一样。它把不在站点主目录下的文件映射到主目录下，以便用户访问。这有助于丰富站点的内容。它的配置格式为：Alias URL-path file-path|directory-path，前面部分 URL-path file-path 代表目录映射到主目录下的文件夹路径，后面部分 directory-path 代表所要映射的目录的实际路径。如 Alias /image grfwgz01://ftp/pub/image，就表示把 grfwgz01 主机 FTP 共享目录下的 image 目录映射成站点服务器主目录下的 image 目录。这样，客户访问这个虚拟目录时就像访问主目录下的 image 目录一样。当然，在配置时还得为用户设置与这个实际目录相应的访问权限，否则用户很可能无法打开所指定的虚拟目录。配置目录的访问权限是通过 Directory 选项进行的，如配置此处 ftp/pub/image 目录的访问权限，就需按如下配置进行。

```
Alias /image grfwgz01://ftp/pub/image
<Directory grfwgz01://ftp/pub/image>
Order allow,deny
Allow from all
</Directory>
```



注意

如果 url-path 中有后缀“/”，则服务器要求有后缀“/”以扩展此别名。也就是说“Alias /icons//usr/local/apache/icons/”并不能对“/icons”实现别名。另外，可能需要额外指定一个<Directory>段来覆盖别名的最终对象。由于只有出现在<Directory>段之前的别名才会被检测，所以它只对最终对象生效。特别要注意，如果对在 DocumentRoot 之外的某个目录建立了一个 Alias，则可能需要明确的对目标目录设定访问权限。

8. ScriptAlias

ScriptAlias 指令的行为与 Alias 指令相同，但同时它又标明此目录中含有应该由 cgi-script 处理器处理的 CGI 脚本。以 URL-path 开头的 URL 会被映射到由第二个参数指定的具有完整路径名的本地文件系统的脚本中。其语法格式为：ScriptAlias URL-path file-path|directory-path，例如：

```
ScriptAlias /cgi-bin/ /web/cgi-bin/
```

这样，对 http://myserver/cgi-bin/foo 的请求会引导服务器执行/web/cgi-bin/foo 脚本。

该指令是设置 CGI 文件的存放路径。CGI 程序的功能类似于 ASP，是一种比较旧的动态网页效果制作技术。虽然现在有了功能更先进的 ASP 或 ASP.NET，它有些过时，但是对于一般企业及个人 Web 服务器来说，它的功能还是足够的。

9. HostnameLookups

该指令启用了 DNS 查询，使得主机名能被记入日志（并用 REMOTE_HOST 变量传递给 CGI/SSI）。其语法格式为：HostnameLookups On|Off|Double，默认值为：Off。参数 Double 指定进行一次双向 DNS 查询。也就是说在一次反向查询之后，再对返回的结果进行一次正向查询。在正向查询结果中至少应该有一个 IP 地址与初始的地址相符。（在“tcpwrappers”中的术语是 PARANOID）。

不论此处如何设置，当使用 mod_authz_host 来根据主机名控制访问的时候，就会执行一

180 网管员必读——网络应用（第2版）

次双向查询。这对安全来说非常必要。请注意，如果没有设置“HostnameLookups Double”，这种双向查询的结果不是自动生成的。比如说，如果仅设置了“HostnameLookups On”而且请求是针对一个主机名做了限制的对象，不论双向查询是否失败，CGI 还是会把单向查询的结果用 REMOTE_HOST 来传送。

默认值设置为 Off，是为了那些不需要进行反向查询的站点节约网络带宽考虑的。这对最终用户也是有益的，因为这样他们就不用忍受查询造成的延迟了。高访问量的网站应该将此指令设置为 Off，因为 DNS 查询会造成明显的时间消耗。在 bin 目录下的 logresolve 工具可以在离线的情况下对已经记入日志的 IP 地址进行主机名的查询。

10. LogLevel

设置日志记录的事件级别，即选择日志启示的事件。它包括的事件有：debug（调试）、info（信息）、notice（通告）、warn（警告）、error（错误）、alert（报警）、emerg（紧急）。配置格式为：LogLevel 日志事件。如 LogLevel warn，则只对报警事件进行记录。如需记录多个事件，多个事件之间用逗号（,）分隔。

因受本书篇幅限制，在此就不再对 Apache 服务器的高级配置进行介绍，有需要的朋友可以参见其他相关书籍或资料。



第 4 章 FTP 站点的配置与管理

Web 网站是用来供用户访问、了解相关信息的，而 FTP 站点是用来与用户共享文件资料的，如提供文件浏览、查阅、上传/下载等。

FTP 站点的组建与网站的组建一样，实现的方式有多种，目前典型的应用方案是微软 Windows 系统中的 IIS 方案和 Server-U 方案。本章要对这两种方案分别予以介绍，其中 IIS 方案中所采用是最新的 Windows Server 2003 R2 系统中的 IIS 6.0 版本。因为在本书第 2 章介绍的 IIS 6.0 基础知识（如 IIS 6.0 的结构和主要改进、IIS 6.0 的安全特性等）同样适用于 IIS 中的 FTP 站点，所以在本章就不再介绍这方面的知识了，有需要的读者请参见第 2 章的相关内容。Serv-U FTP 站点方案是以目前最新的 6.3 版本为例进行介绍的。它的功能要远比 IIS 6.0 中的 FTP 站点功能要强大，所以它也是目前应用最广的 FTP 站点方案。

另外，本章还将介绍 FTP 站点文件上传、下载工具 CutFTP 的基本使用方法。

本章重点

- IIS FTP 站点的创建
- IIS FTP 站点的安全设置
- IIS FTP 虚拟目录和属性配置
- IIS FTP 站点的远程管理方法
- Serv-U FTP 站点的创建（包括两种类型）
- Serv-U FTP 站点用户、组账户的创建和配置
- Serv-U FTP 站点用户主目录的配置
- Serv-U FTP 服务器和域全局设置
- Serv-U FTP 站点虚拟目录和虚拟链接的创建
- CuteFTP 的站点管理和文件上传、下载方法

4.1 利用 IIS 6.0 创建 FTP 站点的基本思路

相对于 IIS 6.0 Web 网站的创建来说，利用 IIS 6.0 创建 FTP 站点要简单许多。以下是利用 IIS 6.0 创建 FTP 站点的基本思路。

（1）安装 IIS 和 FTP 服务所需的组件

这一步也是前提，否则在 FTP 站点建设中所需要用到“Internet 信息服务（IIS）管理器”和 FTP 站点就不会在系统中出现，我们也就无法使用它来建设 FTP 站点了。因为与 IIS 相关的组件安装已在本书的第 2 章有了详细介绍，所以在此仅介绍与 FTP 站点有关的组件安装。

本部分的具体内容参见本章的 4.2 节。

（2）新建 FTP 站点

新建 FTP 站点也是在 IIS 管理器中进行的。FTP 站点创建也可以采取两种方式：一是编辑系统自带的“默认 FTP 站点”；二是重新利用向导新建（可选）。如果公司只需一个 FTP 站点，建议采用编辑系统默认的 FTP 站点方式，所以此步为可选项。

FTP 站点的具体新建步骤参见本章的 4.3 节。

（3）FTP 站点基本信息配置

FTP 站点基本信息的配置包括 FTP 站点名、IP 地址、端口号和站点主目录等。具体参见本章的 4.4 节。

（4）FTP 站点安全配置

同样，FTP 站点的安全配置是指站点的身份验证方式、用户访问权限、数据加密和服务证书等配置。具体参见本章的 4.5 节。

（5）虚拟目录创建与配置（可选）

与 Web 网站一样，在 IIS 的 FTP 站点中，在配置了主目录以后，也可以把位于主目录的站点目录设置为虚拟目录。虚拟目录与站点的配置相似，它也可配置独立的身份验证方式、访问权限等安全选项。但并不是所有 FTP 站点都需要创建和配置虚拟目录，所以为可选项。

具体配置步骤参见本章的 4.6 节。

（6）FTP 站点的管理（可选）

FTP 站点的管理包括站点的启用与停止、主目录的更改、隔离用户、远程管理等。具体参见本章的 4.7 节。

（7）动态域名解析和端口映射配置（可选）

动态域名解析也是针对没有固定外网 IP 地址的对外 FTP 站点而言的，如果 FTP 站点仅用于局域网内部，则无须配置；而端口映射则是针对 FTP 服务器没有直接连接到互联网上，而是通过其他途径共享上网的情况的。具体也请参见本书的第 1 章介绍。

4.2 安装 FTP 服务组件

FTP 服务所需组件的安装与其他 IIS 组件的安装方法是一样的，也是通过控制面板中的“添加或删除程序”功能实现的，所以在此仅说明 FTP 服务组件所在的位置（当然也必须同

时安装 IIS 基本组件，参见第 2 章介绍），具体的步骤在此不做介绍。FTP 服务组件所在的位置如图 4-1 所示，最终安装要选择的是“文件传输协议（FTP）服务”选项。按图中的层叠顺序打开相应的对话框即可看到。

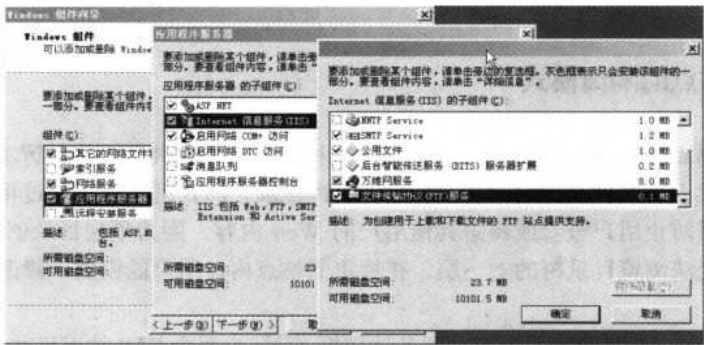


图 4-1 FTP 服务组件位置

安装了 IIS 和 FTP 服务组件后，系统会在 LocalDrive:\inetpub\Ftproot 下创建一个默认的 FTP 目录。打开 IIS 管理器就可以看到系统默认安装的 FTP 站点，如图 4-2 所示。

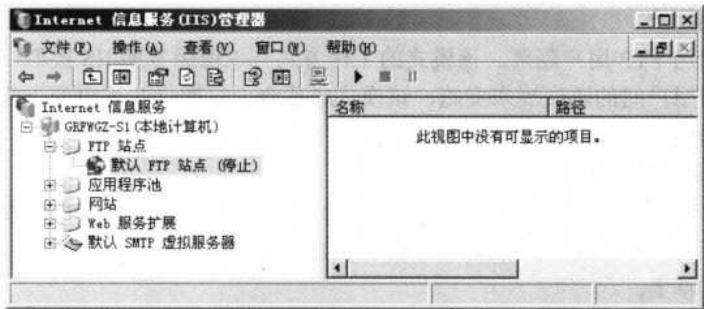


图 4-2 IIS 管理器中默认的 FTP 站点



本来在组件安装后，默认安装的 FTP 站点会自动启用，但是由于笔者当前系统中已安装了其他的 FTP 服务程序，在端口上与 IIS 中的 FTP 站点默认使用的端口（默认为 21 号 TCP 端口）相冲突，所以处于“停止”状态。要重新启动它有两种方法：一是卸载所安装的其他 FTP 服务程序如 Serv-U（仅关闭程序没有用），或者关闭在“服务”窗口中其他 FTP 程序的相关服务器（如 Serv-U 程序中自动添加的“Serv-U FTP Server”服务）；二是把两个 FTP 服务程序中所用的端口号改为不一致。采用以上任意一种方法都可以重新启动 IIS 中的 FTP 站点。

4.3 新建 FTP 站点

在 4.1 节就介绍了，新建 FTP 站点的方法可以两种：一是通过编辑修改系统默认安装的“默认 FTP 站点”（参见图 4-2）配置来实现，这一般适用于用户只需一个 FTP 站点的情况

下；二是如果用户需要多个站点，则必须采取向导方式来创建。因为编辑“默认 FTP 站点”的方式与本章后面将要介绍的 FTP 站点配置方法基本一样，所以在此仅对向导新建方式进行介绍。因为涉及到 3 种不同的隔离模式，所以本节分别予以介绍。先来了解有关 FTP 站点的隔离模式。

4.3.1 FTP 站点的隔离模式

FTP 用户隔离为 Internet 服务提供商（ISP）和应用服务提供商提供了解决方案，使他们可以为客户提供上载文件和 Web 内容的个人 FTP 目录。FTP 用户隔离通过将用户限制在自己的目录中，以防止用户查看或覆盖其他用户的 Web 内容。因为顶层目录就是 FTP 服务的根目录，用户无法浏览目录树的上一层。在特定的站点内，用户能创建、修改或删除文件和文件夹。

FTP 用户隔离是站点属性，而不是服务器属性。无法为每个 FTP 站点启动或关闭该属性，所以这一属性在创建 FTP 站点时配置，一旦配置就无法改变。

1. FTP 站点的 3 种隔离模式

FTP 用户隔离支持 3 种隔离模式，每一种模式都会启动不同的隔离和验证等级。

■ 不隔离用户

该模式不启用 FTP 用户隔离。该模式的工作方式与以前版本的 IIS 类似。由于在登录到 FTP 站点的不同用户间的隔离尚未实施，该模式最适合于只提供共享内容下载功能的站点或不需要在用户间进行数据访问保护的站点。

■ IIS 管理器隔离用户

当设置 FTP 服务器使用隔离用户时，所有的用户主文件夹都在 FTP 站点目录中的二级目录结构下（如，FTP“主目录”属性页中配置的那样）。FTP 站点目录可以在本地计算机上，也可以在网络共享上。

该模式在用户访问与其用户名匹配的主目录前，根据本机或域账户验证用户。所有用户的主目录都在单一 FTP 主目录下，每个用户均被安放和限制在自己的主目录中。不允许用户浏览自己主目录外的内容。如果用户需要访问特定的共享文件夹，可以再建立一个虚拟根目录。该模式不使用 Active Directory 目录服务进行验证。

■ 用 Active Directory 隔离用户

该模式根据相应的 Active Directory 容器验证用户凭据，而不是搜索整个 Active Directory，那样做需要花费大量的处理时间。Active Directory 将为每个客户指定特定的 FTP 服务器，以确保数据的完整性及隔离性。当用户对象在 Active Directory 容器内时，可以将 FTPRoot 和 FTPDir 属性提取出来，为用户主文件夹提供完整路径。如果 FTP 服务能成功地访问该路径，则用户被放在代表 FTP 根位置的该主目录中。用户只能看见自己的 FTP 根位置，因此，受限制而无法向上浏览目录树。如果 FTPRoot 或 FTPDir 属性不存在，或它们无法共同构成有效、可访问的路径，那么用户将无法访问。

在 FTP 服务器上使用 Active Directory 隔离用户时，每个用户的主目录均可放置在任意的网络路径上。在此模式中，可以根据网络配置情况，灵活地将用户主文件夹分布在多个服务器、多个卷和多个目录中。可以设置 FTPRoot 和 FTPDir 属性，以使用户建立到 FTP 服务

器的本地路径。该模式在检索用户主文件夹信息时，集成了 Active Directory 验证。这种集成可以通过 Active Directory 服务界面（ADSI）和编写脚本来管理用户主文件夹的物理位置。

2. “Active Directory 隔离用户”模式特性

该模式最适合 ISP 部署，这些部署前端 FTP 服务器集都通过访问 Active Directory 来检索用户主文件夹信息，然后访问后端文件服务器集。

Active Directory User 对象经过扩展，包括两个属性：FTPRoot 和 FTPDir。这些属性为每个用户保存文件服务器共享和相对主目录。FTPRoot 决定通用命名规范（UNC）文件服务器共享，而 FTPDir 则用来指出共享的相对路径。合并这两种属性可以产生到用户主文件夹或 FTP 服务器的 UNC 完整路径。

这两种属性对应于在 Windows Server 2003 家族的 Active Directory 架构中添加的 msIIS-FTPRoot 和 msIIS-FTPDir 属性，也可以使用 iisftp.vbs 命令行管理脚本设置并修改它们。还可以安装 Admin Pack（可在 Windows Server 2003 家族资源工具包中找到），然后使用 Active Directory 管理单元修改这些属性。

使用 Active Directory 配置用户隔离涉及到设置如下相关服务。

- 文件服务器：可以使用文件服务器为所有允许连接 FTP 服务的用户（包括匿名账户）创建共享和用户目录。应该考虑预计磁盘空间的使用、存储管理、网络流量及其他与服务器基础结构有关的过程。
- Active Directory：该用户隔离模式需要在 Windows Server 2003 家族中的操作系统上运行 Active Directory 服务器。Windows Server 2003 家族 Active Directory 架构最先包含 FTP 服务使用的用户对象属性。还可以通过设置指向主目录的 FTPRoot 和 FTPDir 属性，为每个用户（包括匿名账户）在 Active Directory 中配置用户对象。需要注意的是，经常使用的用户信息将从 Active Directory 中检索出来，并写入 FTP 服务器的缓存中，也可以在使用注册表参数 DsCacheRefreshSecs 刷新缓存中与匿名用户对应的 Active Directory 属性之前，限制最大运行时间。



在使用“不隔离用户”模式创建了上百个主目录时，服务器性能会下降。而选择“用 Active Directory 隔离用户”模式时，需要在 Windows Server 2003 家族的操作系统上运行 Active Directory 服务器。也可以使用 Windows 2000 Active Directory，但是需要手动扩展 User 对象架构。

另外，FTP 用户隔离的是站点属性，而不是服务器属性。无法为每个 FTP 站点启动或关闭该属性，也无法在站点创建后再进行配置，所以，如果确定要选择某种隔离模式，就一定要在具体站点创建前选定。

另外，在 IIS 6.0 中这 3 种不同隔离模式的 FTP 站点的配置方法存在很大不同，而且后面两种隔离用户模式的配置还存在着很深的技巧，在系统的帮助说明中只是很简单的提到，并没有具体说明如何配置。不搞清楚这些隔离用户模式的 FTP 站点配置也就无法创建，更无法实现 FTP 站点的访问。所以下面几节介绍的内容大家要仔细看清楚后面的配置。

4.3.2 无隔离用户的 FTP 站点创建

这种无隔离用户的 FTP 站点创建是最简单的，也无须特别配置。它特别适用于对外提供所有用户均共享相同文件的公共服务的 FTP 站点。下面是利用新建 FTP 站点向导创建无隔离用户的 FTP 站点的具体步骤。

(1) 在如图 4-2 所示的 IIS 管理器主界面的“FTP 站点”容器上单击鼠标右键，在弹出的快捷菜单中选择“新建”下的“FTP 站点”选项，打开如图 4-3 所示的向导对话框。

(2) 单击【下一步】按钮，打开如图 4-4 所示的对话框。在“描述”文本框中输入 FTP 站点的描述（其实就是站点的标识名称），本示例为“grfwgz”。

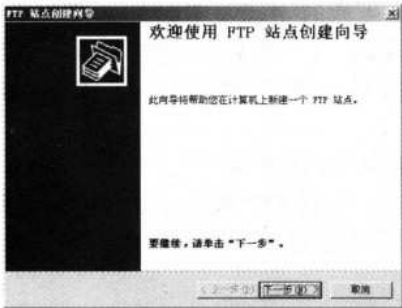


图 4-3 “欢迎使用 FTP 站点创建向导”对话框

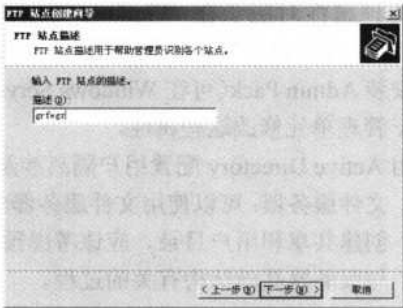


图 4-4 “FTP 站点描述”对话框

(3) 单击【下一步】按钮，打开如图 4-5 所示的对话框。在这里要为新建的 FTP 站点指定 IP 地址和端口。一般来说，FTP 站点的标识有两种方式：IP 地址和 TCP 端口（Web 站点还有一种“主机头”标识法）。这两者之中只要有一个不同即可，所以，即使同一个 IIS 管理器中有多个 FTP 站点，只要 IP 地址或者端口号不一样，就可以同时运行。不过，一般来说，FTP 的 21 号端口不宜更改，因为它是默认端口，否则容易引起不能访问的故障，因为通常的访问是不带端口号的。

(4) 单击【下一步】按钮，打开如图 4-6 所示的对话框。在这个对话框中要选择用户隔离模式。FTP 用户隔离支持 3 种隔离模式。每一种模式都会启动不同的隔离和验证等级。在此先选择“不隔离用户”单选项。



图 4-5 “IP 地址和端口设置”对话框

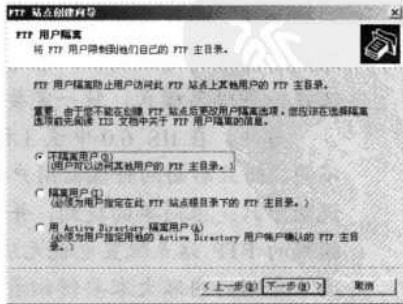


图 4-6 “FTP 用户隔离”对话框

(5) 单击【下一步】按钮，打开如图 4-7 所示的对话框。在这个对话框中要指定 FTP

站点主目录。这时要选择供用户共享使用的根目录路径，系统默认的路径为 Inetpub\ftproot，如果在同一 IIS 中已有 FTP 站点使用了这个默认目录，则不能再使用了，需要另外创建，但仍可以在 Inetpub 目录下，且应注意在 NTFS 格式磁盘中。当然也可以使用本机或网络中其他任何 NTFS 格式目录。可直接在“路径”文本框中输入，也可通过单击【浏览】按钮，在打开的对话框中查找定位。直接输入时，如果主目录在网络的其他计算机上，则一定要采用 UNC 共享路径格式（\\server\sharename）。

(6) 选择好后，单击【下一步】按钮，打开如图 4-8 所示的对话框。在这里要选择 FTP 站点允许用户访问时所允许的权限。通常只需选择“读取”复选项即可。但如果要允许多个用户上传文件，则还需要选择“写入”复选项。不过，这里设置的是普通用户的访问权限，所以只选择“写入”复选项，对于管理员或者操作员来说，需要上传文件，则可通过具体用户的 NTFS 文件访问权限来实现，具体将在本章后面的 FTP 站点配置中介绍。

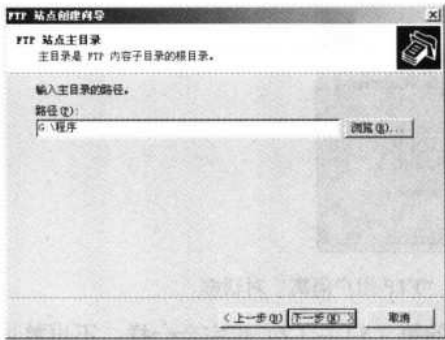


图 4-7 “FTP 站点主目录”对话框

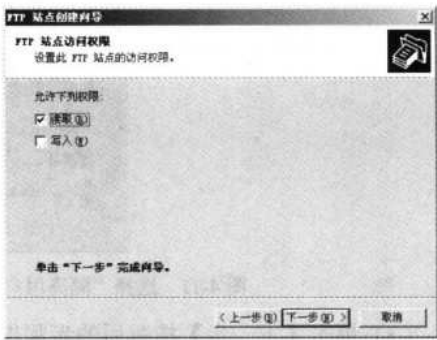


图 4-8 “FTP 站点访问权限”对话框

(7) 单击【下一步】按钮，打开如图 4-9 所示的向导完成对话框。直接单击【完成】按钮即可完成整个创建向导。完成后，在 IIS 管理器中就能看到新建的 FTP 站点，如图 4-10 所示。

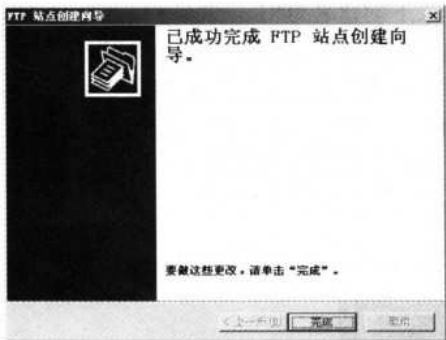


图 4-9 “已成功完成 FTP 站点创建向导”对话框

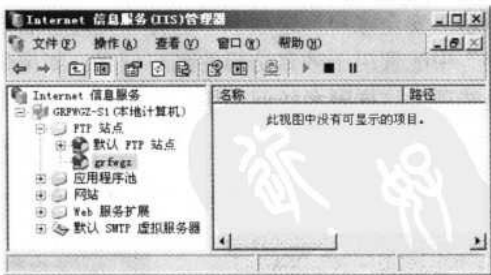


图 4-10 新建 FTP 站点后的 IIS 管理器界面

对于无隔离用户的 FTP 站点无须特别的配置，只需按照本章后面介绍的基本通用配置方法配置相应的访问权限及其他基本信息即可。下面着重介绍后面两种隔离用户模式的 FTP 站点创建与配置。

4.3.3 IIS 管理器隔离用户 FTP 站点创建与配置

使用 IIS 管理器隔离用户是 FTP 站点的一种主要隔离模式，主要应用在 FTP 站点为不同用户提供不同的共享文件内容时。它的适用性比后面将要介绍的“Active Directory 隔离用户”模式要广，配置也相对容易些。

1. FTP 隔离用户站点创建

具体步骤如下。

(1) 前面的步骤参见 4.3.2 的第 (1) ~ (3) 步。

(2) 在 4.3.2 的第 (4) 步中，当出现图 4-6 所示的对话框时，要选择“隔离用户”单选项，如图 4-11 所示。

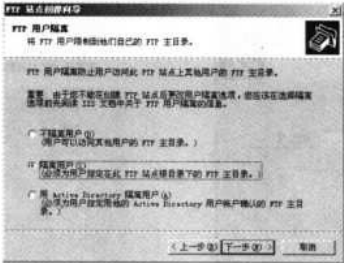


图 4-11 选择“隔离用户”项时的“FTP 用户隔离”对话框

(3) 单击【下一步】按钮后的步骤也与上节的第 (5) ~ (7) 步完全一样，不再赘述。

但通过这种方式创建的 FTP 站点如果不经进一步的配置，用户是无法访问的，匿名访问也不行，即使是配置了该 FTP 站点允许匿名访问也不能使用。

2. IIS 隔离用户模式的 FTP 站点需要做进一步的配置

(1) 如果要允许匿名访问，请在 FTP 站点主目录下创建名为“LocalUser”和“LocalUser\Public”子目录（注意，这两个目录名不能改）。此时需在相应 FTP 站点属性对话框如图 4-12 所示“安全账户”选项卡中选择“允许匿名连接”复选项，并且在下面的“用户名”和“密码”中配置用于匿名访问的账户信息。如果仅允许匿名访问，还要选择“只允许匿名连接”复选项。这样匿名访问的用户就能直接进入到这个 public 子目录下。

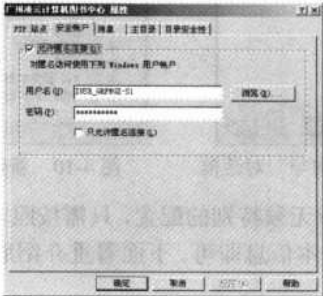


图 4-12 FTP 站点属性对话框“安全账户”选项卡

允许匿名访问时，用户连接 FTP 站点不会弹出身份验证对话框，将直接进入 public 公用目录下。

(2) 如果要使用域用户访问 FTP 站点，则要在如图 4-12 所示的对话框中取消“允许匿名连接”复选项。然后在 FTP 主目录下创建以相应域名为文件夹名的目录，如本例中的域为 grfw（无须尾缀），则需在 FTP 主目录下创建 grfw 目录。

(3) 然后继续在相应域名目录下为各用户创建用户访问 FTP 站点时的主目录，主目录名也与相应用户名一样。如 winda 用户的 FTP 站点 winda 主目录名也为 winda。这样，用户的访问就直接进入相应用户的主目录下，而不能进入其他目录，达到用户隔离的目的。

要使用用户账户凭据连接 FTP 站点时，会弹出如图 4-13（a）所示的身份验证对话框。并显示不支持匿名访问，即使在对话框中选择“匿名登录”复选项也不行。此时只能在“用户名”和“密码”两个文本框中输入域用户账户信息。当然，所输入的用户账户必须有权访问相应用户主文件夹，具体访问权限的配置将在本章后面详细介绍。但前提是必须按以上的方法配置 FTP 站点主目录下以域命名的目录和以相应用户账户命名的账户子目录才可访问，否则无法登录成功，返回“用指定的用户名和密码无法登录到该 FTP 服务器”的错误提示（如图 4-13（b）所示），即使是管理员也不例外。

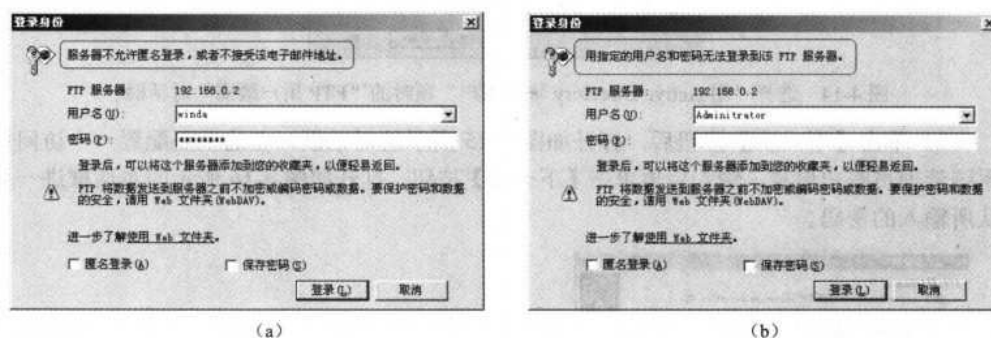


图 4-13 “登录身份”对话框

4.3.4 Active Directory 隔离用户 FTP 站点的创建

使用“Active Directory 隔离用户”选项会为使用者导入一个数据夹。这个数据夹是由 Active Directory 内的“msIIS-FTPRoot”和“msIIS-FTPDDir”属性定义的，而且会在使用者工作阶段中成为 FTP 网站的根目录。使用者无法回到 FTP 网站实际的主目录。

在这种模式下，Active Directory 服务器必须在 Windows Server 2003 系列产品的操作系统中执行。也可以使用 Windows 2000 Active Directory，但需要手动延伸使用者对象结构描述，因为它在 Windows 2000 Active Directory 中无法还原。建议代管服务供货商和需要维护大量 FTP 使用者数据夹的公司使用 Active Directory 进行使用者隔离。

必须指派 FTP 主目录给使用者，而且主目录必须以使用者自己的 Active Directory 使用者账户进行设定。要验证使用者的主数据夹，需要查询 Active Directory 中使用者对象的 msIIS-FTPRoot 和 msIIS-FTPDDir 属性即可。msIIS-FTPRoot 和 msIIS-FTPDDir 所串联的值即形成使用者主数据夹的路径。

举例来说：msIIS-FTPRoot = D:\FTP Users；msIIS-FTPDDir = \winda，如此，即产生使用者的主数据夹“D:\FTP Users\winda”。

先介绍用 Active Directory 隔离用户的 FTP 站点的创建步骤。

1. 创建用 Active Directory 隔离用户的 FTP 站点

具体步骤如下。

(1) 前面的步骤参见 4.3.2 的第 (1) ~ (3) 步。

(2) 在 4.3.2 节的第 (4) 步，当出现图 4-6 所示的对话框时，要选择“用 Active Directory 隔离用户”单选项，如图 4-14 所示。

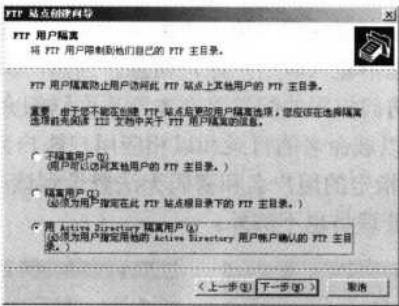


图 4-14 选择“用 Active Directory 隔离用户”项时的“FTP 用户隔离”对话框

(3) 单击【下一步】按钮后，打开如图 4-15 所示的对话框。在这里要配置一个访问域的系统管理员账户信息。输入后再单击【下一步】按钮，打开如图 4-16 所示的对话框进一步确认所输入的密码。



图 4-15 配置用户账户信息对话框

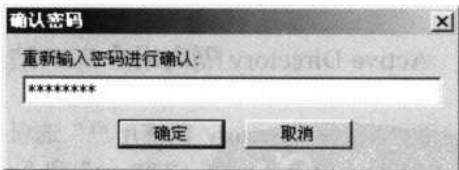


图 4-16 “确认密码”对话框

(4) 单击【确定】按钮后弹出如图 4-9 所示的向导完成对话框。单击【完成】按钮完成 FTP 站点的创建。

从以上步骤可以看出，在“用 Active Directory 隔离用户”的 FTP 站点创建中，是不用指定 FTP 站点主目录的。这个主目录及 FTP 站点的用户主文件夹均需通过本节后面介绍的方法来配置。

2. 配置用 Active Directory 隔离用户的 FTP 站点

基于 ActiveDirectory 的用户活动隔离用于承载提供和公司需要维护大量的 FTP 用户

文件夹。当用户的主文件夹验证时，由查询 msIIS-FTPRoot 和 FTPDir msIIS-Active Directory 中的用户对象属性来决定。msIIS-FTPRoot 和 msIIS-FTPDir 的串联结果可用到用户的主文件夹路径中。如 FTPRoot msIIS = D:\FTP Users; msIIS-FTPDir = \winda，这样“D:\FTP Users\winda”就作为 winda 用户的主文件夹。

可使用命令行脚本 iisftp.vbs（存储在 systemroot\System32 中）查询和设置用户的 FTP 站点主目录的 Active Directory 目录服务属性。不过，此时必须是本地计算机上 Administrators 组的成员或者必须被委派了相应的权限，才能运行脚本和可执行文件。作为安全性的最佳操作，请使用不属于 Administrators 组的账户登录计算机，然后使用运行方式命令以管理员身份运行脚本或可执行文件

基本语法格式为：iisftp /GetADProp UserID [/s Computer [/u [Domain\]User/p Password]]

或：iisftp /SetADProp UserID {FTPDir|FTPRoot} PropertyValue [/s Computer [/u [Domain\]User/p Password]]

参数说明如下。

- /GetADProp: 返回特定 Active Directory 用户的属性值。
- /SetADProp: 设置特定 Active Directory 用户的属性值。
- UserID: 必需的。指定 Active Directory 用户的登录 ID。
- FTPDir|FTPRoot: 设置主目录属性所必需的。在目录级别或根目录级别指定隔离。
- PropertyValue: 设置主目录属性所必需的。指定主目录和相对路径的值。
- /s Computer: 指定远程计算机的名称或 IP 地址（不带反斜杠）。默认值是本地计算机。
- /u [Domain\]User: 以 user 或 domain\user 格式的指定用户账户的权限连接到 Active Directory。该账户必须是远程计算机上 Administrators 组的成员。在默认情况下，脚本使用本地计算机当前用户的权限运行。
- /p Password: 指定在/u 参数中指定的用户账户的密码。

由 Active Directory 隔离了用户的 FTP 站点创建好后，就只需要设置 Active Directory 的 msIIS-FTPRoot 和 msIIS-FTPDir 属性。方法是使用 iisftp /SetADProp 命令，如要设置 winda 用户的 FTPRoot 属性，则在命令提示符状态下输入如下命令：

```
iisftp /SetADProp winda FTPRoot d:\inetpub\ftproot\
```

要设置 winda 用户的 FTPDir 属性，则在命令提示符状态下输入如下命令：

```
iisftp /SetADProp winda FTPDir d:\inetpub\ftproot\winda
```

如果事先没有注册 CScript 脚本，在输入以上命令行时，系统会弹出如图 4-17 所示提示框。单击【确定】按钮，又弹出如图 4-18 所示提示框，提示是否马上注册。单击【是】按钮，系统自动注册，成功后又弹出如图 4-19 所示的提示框。

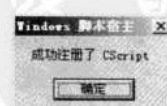
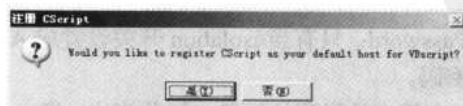
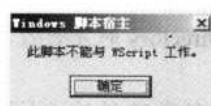


图 4-17 “Windows 脚本宿主” 提示框

图 4-18 “注册 CScript” 提示框

图 4-19 成功注册提示框

4.3.5 使用命令行脚本 iisftp.vbs 创建 FTP 站点

相对于上面介绍的界面方式来说，在创建隔离模式的 FTP 站点时，使用命令行脚本 iisftp.vbs 的方式显得更简单、有效。

使用命令行脚本 iisftp.vbs（存储在 systemroot\System32 中），在运行带有 IIS 6.0 的 Windows Server 2003 家族成员的本地或远程计算机上，创建文件传输协议（FTP）站点配置。该命令并不创建或破坏内容，但它会设置目录结构和 IIS 配置文件。

在使用 iisftp.vbs 创建新的 FTP 站点时，只指定创建站点和标识其内容所需的基本属性。iisftp.vbs 使用的默认属性与 IIS 管理器在建立新的 FTP 站点时使用的属性相同，并且它遵循相同的继承属性规则。要配置 FTP 站点的更多高级属性，请使用 IIS 管理器。

基本语法格式如下：

```
iisftp /create Path SiteName [/b Port] [/i IPAddress] [/dontstart] [/isolation {ActiveDirectory | Local}
[/domain DomainName /Admin [Domain\]User /AdminPwd Password]] [/s Computer [/u [Domain\]
User /p [Password]]]
```

参数说明如下。

- Path: 指定 FTP 站点内容文件的位置。路径必须是本地路径，如 C:\Projects\HTML。如果指定的路径不存在，iisftp.vbs 就会创建该路径。

在命令中，Path 参数必须紧跟在 SiteName 参数前面。否则，iisftp.vbs 不能正确地解释站点信息。

- SiteName: 必需的。指定 FTP 站点的名称。
- /b Port: 指定 FTP 站点的 TCP 端口号。默认值为 21。
- /i IPAddress: 指定 FTP 站点的 IP 地址。默认值是“All Unassigned”（所有未分配），这将为该站点指派未分配给其他站点的计算机上的所有 IP 地址。每个 IIS 服务器上只能有一个站点设置为“所有未分配”。
- /dontstart: 表明 FTP 站点不会在创建后很快就自动启动。在默认情况下，当/create 命令成功完成时，IIS 将启动 FTP 站点。
- /isolation {ActiveDirectory | Local}: 提供了下面两个用户隔离模式中的一个：AD（Active Directory）和“Local”。如果/isolation 开关不存在，则该站点将不使用用户隔离。
- /domain DomainName: 只有当/isolation 开关设置成 Active Directory 时才有效，该值是 Active Directory 域的名称。
- /Admin [Domain\]User: 只有当/isolation 开关设置成 Active Directory 时才有效，该值是 User、Domain\User 或 User@Domain 格式中的管理员的名称。
- /AdminPwd Password: 只有当/isolation 开关设置成 Active Directory 时才有效，该值是管理员的密码。
- /s Computer: 在指定的远程计算机上运行脚本。键入计算机名或 IP 地址（不带反斜杠）。在默认情况下，将在本地计算机上运行脚本。
- /u [Domain\]User: 使用特定用户账户的权限运行脚本。该账户必须是远程计算机上

Administrators 组成员。在默认情况下，脚本使用本地计算机上当前用户的权限运行。

- /p Password: 指定在/u 参数中指定的用户账户的密码。如果忽略该参数，脚本将提示输入密码并隐藏键入的文本。
- /?: 在命令提示符下显示帮助。



iisftp.vbs 不验证 FTP 站点的端口号或 IP 地址，并且它并不验证这些绑定在服务器内是否为唯一的。如果用无效的或发生冲突的绑定创建站点，则站点将不启动。

如下是几个示例。

示例 1：在本地计算机上创建“Archives”FTP 站点，并将它的主目录设为 D:\Public\Archives。Archive 为运行脚本的账户，此命令忽略所有的可选参数并接受默认值。“Archives”子目录不存在，因此，iisftp.vbs 将在“Public”目录中创建该子目录。命令行如下：

```
iisftp /create D:\Public\Archives Archive
```

作为响应，iisftp 显示以下消息及新 FTP 站点的基本属性。在本示例中，“Server”表示在其中找到驱动器 D:的计算机名，“SiteName”是为 FTP 站点指定的名称，“Metabase Path”表示 IIS 指定的配置数据库项（它与系统注册表中的注册表项类似），“IP”默认情况下是未分配的，“Port”默认情况下设置为 21，“Root”是 FTP 文件所在的目录，默认情况下将“Status”设置为“STARTED”。

```
正在连接到服务器...已完成。
Server = RESKIT
SiteName = Archive
Metabase Path = MSFTPSVC /1452008083
IP = ALL UNASSIGNED
Port = 21
Root = D:\Public\Archives
Status = STARTED
```

示例 2：在远程服务器上创建“Drivers”FTP 站点配置。站点的主目录为 SVR16 上的 C:\Public\Download 目录。此命令使用/i 参数指定站点的 IP 地址为 172.31.69.150，并使用 /dontstart 参数防止站点自动启动。它使用/s 参数来指定远程计算机，使用/u 和/p 参数以用户的管理员账户权限运行脚本。命令行如下：

```
iisftp /create C:\Public\Download Drivers /i 172.31.69.150 /dontstart /s SVR16 /u Admin6 /p p@ssWor#
```

作为响应，iisftp 显示以下消息及新 FTP 站点的基本属性。在本示例中，“Server”表示服务器计算机，“SiteName”表示 FTP 站点指定的名称，“Metabase Path”表示 IIS 指定的配置数据库项（它与系统注册表中的注册表项类似），“IP”表示指定的 DNS 地址，“Port”默认情况下设置为 21，“Root”是 FTP 文件所在的目录，根据需要将“Status”设置为“STOPPED”。

```
正在连接到服务器...已完成。
Server = SVR16
SiteName = Drivers
Metabase Path = MSFTPSVC /1932955329
IP = 172.31.69.150
```


194 网管员必读——网络应用（第2版）

```
Port = 21
Root = C:\Public\Download
Status = STOPPED
```

示例 3：域系统管理员在本地计算机的本地域上创建用 Active Directory 隔离的 FTP 站点 grfw。站点主目录为本地计算机 grfwgz-s1 上的 d:\inetpub\ftproot。此命令使用/i 参数指定站点的 IP 地址为 192.168.0.8，并使用/dontstart 参数防止站点自动启动。命令行如下：

```
iisftp /create d:\inetpub\ftproot grfw /i 192.168.0.8 /dontstart /isolation ad
```

输入命令行后，系统自动创建由 Active Directory 隔离用户的 FTP 站点，最终显示“已完成的状态”，如图 4-20 所示。

创建完成后，可以在 IIS 管理器中进行一些高级配置，然后启动该 FTP 站点。



图 4-20 以脚本命令行的方式创建 Active Directory 隔离用户模式 FTP 站点后的界面

4.4 FTP 站点基本配置

本节所介绍的基本信息配置包括 FTP 站点所用 IP 地址、TCP 端口、主目录和各种标题配置等。如果采用的是上节介绍的向导方式来创建新的 FTP 站点，则本节可略过，因为在创建向导中就已配置好了基本信息。本节仅针对通过编辑系统默认安装的“默认 FTP 站点”属性来创建 FTP 站点的情形，当然如果要更改通过向导方式创建的新 FTP 站点属性，下面介绍的方法同样适用。



与网站的配置一样，本节和下节的相关配置也可以直接在“FTP 站点”文件夹中配置一些共有信息，如 FTP 站点连接限制、日志格式、安全账户、消息、主目录的访问权限和目录的安全性等，方法是在“FTP 站点”文件夹上单击鼠标右键，在弹出的快捷菜单中，选择【属性】命令，在打开的“属性”对话框中进行配置。这样可适用于该文件夹下的所有 FTP 站点。如果要对具体的 FTP 站点进行设置，则必须在相应的 FTP 站点上单击鼠标右键，在弹出的快捷菜单中，选择【属性】命令，在打开的对应 FTP 站点“属性”对话框中进行配置。在此仅以具体 FTP 站点的配置为例进行介绍。

下面是具体的步骤。

- (1) 在如图 4-10 所示 IIS 管理器中的相应 FTP 站点上单击鼠标右键，在弹出的快捷菜

单中选择【属性】命令，在打开的对话框中选择“FTP 站点”选项卡，如图 4-21 所示（这是“默认 FTP 站点”的相应属性对话框）。

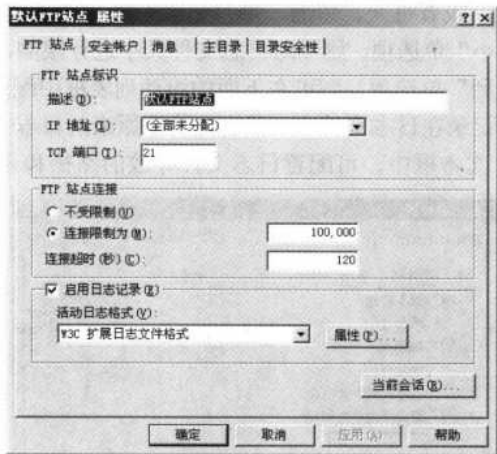


图 4-21 “默认 FTP 站点属性”对话框“FTP 站点”选项卡

（2）在“描述”文本框中可以改为自己需要的描述，其实就是一个名称标识；在“IP 地址”下拉列表框中，“默认 FTP 站点”是选择“全部未分配”选项的，而且在“TCP 端口”文本框中采用的是 FTP 服务默认的 21 号端口。这样，这个站点就适用于当前服务器上所有的 IP 地址，用户只要连接到该服务器 FTP 站点时采用的是 21 号端口，都会打开这个默认 FTP 站点。如果系统中有多个 FTP 站点，显然是不行的，此时就得指定一个唯一的 IP 地址，或者更改所用的 TCP 端口。但通常是采用指定唯一 IP 地址的方式，因为默认的端口号最好不要改，否则很可能访问不了 FTP 站点，因为 FTP 服务默认使用的端口就是 21 号。如果硬是要通过更改端口号来达到标识的目的，则端口号建议在 5 000 以上，因为这个段的端口一般没有分配给特定的服务使用，不会与其他应用程序发生冲突。

如果要限制同一时刻连接的最多用户数，则还可选择“连接限制为”单选项，然后在其后的文本框中设置最多并发连接用户数（默认为 100 000 个），这主要根据 FTP 服务器的硬件配置，实际用户数，以及网络带宽等方面而定。“连接超时”文本框中可以设置用户的最长连接等待时间（默认为 120 秒）。

选择“启用日志记录”复选项可以启用 FTP 站点的日志功能，它可以记录关于用户活动的细节并按所选格式创建日志。信息存储在 ASCII 文件或 ODBC 兼容的数据库中。IIS 中的日志记录信息超出 Windows 系统事件日志，或性能监视器功能的范围。日志包括的信息诸如，哪些用户访问了你的站点、访问者查看了什么内容，以及最后一次查看该信息的时间。可以使用日志来评估内容受欢迎程度或识别信息瓶颈。可以在“活动日志格式”下拉列表框中选择一种日志文件格式。

- Microsoft IIS 日志文件格式：一种固定的 ASCII 格式。
- ODBC 日志记录：一种记录到数据库的固定格式，与该数据库兼容。
- W3C 扩展日志文件格式：一种可自定义的 ASCII 格式，在默认情况下选择此格式。要使用进程记账，必须选择 W3SVC 扩展日志文件格式。

选择一种日志格式后，单击后面的【属性】按钮，打开如图 4-22 所示的对话框（选择“W3C 扩展日志文件格式”时与选择其他格式时所打开的对话框不一样）。在这里，可以配置日志计划（例如每小时记录一次，或者每天、每周、每月记录一次），还可配置日志文件的大小，如果选择了“不限制文件大小”单选项，则不对日志文件大小进行限制，仅受磁盘空间限制；如果选择了“当文件大小达到”单选项，则可在下面的滚动列表框中配置最大的日志文件大小，到达这个值后，日志不再记录在日志文件中，只有先清除原来的日志文件后才可继续记录。

在“日志文件目录”文本框中，可配置日志文件存放的路径和日志文件名。

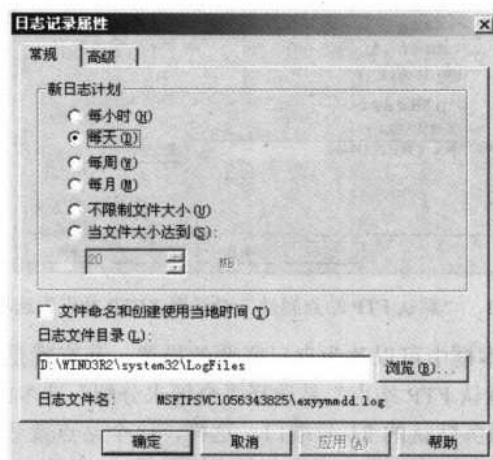


图 4-22 “日志记录属性”对话框“常规”选项卡

选择“文件命名和创建使用当地时间”复选项可以使用本地午夜时间设置 W3C 扩展日志文件的创建时间和命名格式，而不使用格林威治时间。如果在如图 4-21 所示的对话框“活动日志格式”下拉列表框中选择的是 IIS 日志文件格式，则打开的对话框与图 4-22 类似，只是没有“文件命名和创建使用当地时间”复选项，也没有“高级”选项卡，如图 4-23 所示。在这里可以配置 W3C 扩展格式的高级扩展属性。因为通常很少需要配置，所以在此不再介绍。

（3）在如图 4-21 所示的对话框中选择“主目录”选项卡，如图 4-24 所示。在这里可重新配置 FTP 站点的主目录。系统默认配置的“默认 FTP 站点”主目录是在本地计算机中的 inetpub 目录下的 ftproot 目录。也可以继续使用这个目录作为新 FTP 站点的主目录，但必须把相应的 FTP 站点文件全部复制或者移动到这个目录下。当然，也可以选择其他的目录作为主目录，选择此“计算机上的目录”单选项，然后直接在“本地路径”后面的文本框中输入，或者通过单击【浏览】按钮定位即可。这样可以允许用户访问此计算机上的指定目录，以便查看或更新 FTP 内容。可以通过执行任何 Windows 安全方法（如 NTFS 访问权限）来控制对内容的访问。此时，需在“本地路径”文本框中键入目录或目标 URL 的路径。语法必须与当前所选的路径类型相匹配。对于本地目录，请使用完整路径，例如 D:\inetpub\ftproot。

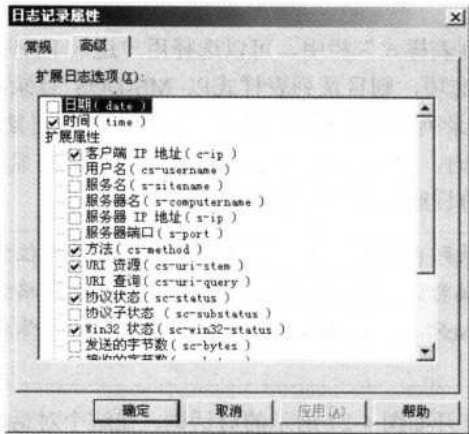


图 4-23 “高级”选项卡

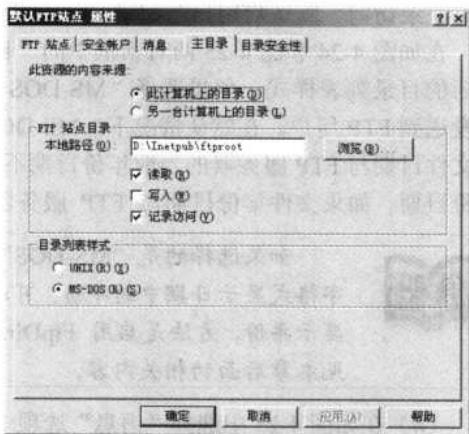


图 4-24 “主目录”选项卡

FTP 站点主目录还可以在网络中的其他计算机上，此时要选择“另一台计算机上的目录”单选项，允许用户查看或更新与该计算机有活动连接的其他计算机上的 FTP 内容。“主目录”选项卡中的选项相应发生了一些改变，如 4-25 所示。

此时，这个要设为主目录的目录一定要在对应计算机上设为共享，然后在如图 4-25 所示的对话框“网络共享”后面的文本框中输入该目录的共享路径和共享名，对于网络共享，请使用通用命名约定（UNC）服务器和共享名，例如\\Webserver\\htmlfiles。或者单击【连接为】按钮，打开如图 4-26 所示的对话框，连接到对方计算机上定位查找。

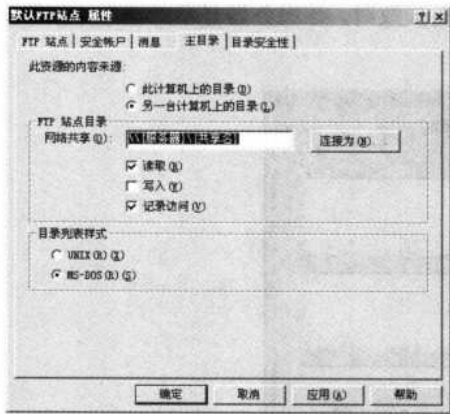


图 4-25 当选择“另一台计算机上的目录”

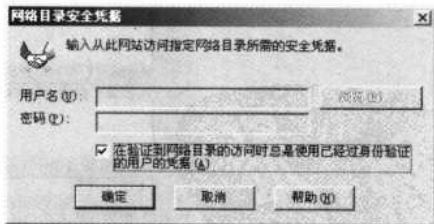


图 4-26 “网络目录安全凭据”对话框

在如图 4-24 和图 4-25 两对话框中部的“读取”、“写入”、“记录访问”这 3 个主目录访问权限复选项是一样的。具有“读取”权限的用户可以读取 FTP 服务器主目录的文件，若要允许用户读取或下载存储在主目录或虚拟目录中的文件，请选择此复选项。而具有“写入”权限的用户则可以在 FTP 服务器上对文件和目录进行编辑，通常具有上传文件权限的用户才可具有，若要允许用户将文件上传到服务器上已启用的目录中，请选中此复选框。具有“记录访问”权限的用户可在日志文件中记录对目录的访问。仅当此 FTP 站点启用日志记录时，

才可记录访问。默认启用日志记录。

在如图 4-24 和图 4-25 两对话框中的“目录列表样式”栏中，可以选择用户进入 FTP 站点后的目录列表样式。如果选择“MS-DOS”单选项，则目录列表样式以 MS-DOS 目录格式发送到 FTP 用户。在默认情况下，MS-DOS 目录列表样式以两位数字格式显示年份日期。当文件日期与 FTP 服务器的当前年份日期不一致时，UNIX 目录列表样式就以四位数字显示年份日期。如果文件年份日期与 FTP 服务器年份日期相同，将不返回年份日期。



如果选择的是“MS-DOS”目录列表样式，则可以在默认情况下用两位数字格式显示日期中的年份。可以以编程方式更改此设置，以便以四位数字格式显示年份，方法是启用 FtpDirBrowseShowLongDate 配置数据库属性。具体参见本章后面的相关内容。

(4) 在如图 4-25 中选择“消息”选项卡，打开如图 4-27 所示的对话框。在这个对话框中我们可以设置用户登录该 FTP 站点时的界面显示，如 FTP 站点标题、用户登录时的欢迎词、用户退出时的欢送词、当用户试图连接站点，但 FTP 站点的当前工作连接用户数已达到规定的极限时所显示的信息。

在“标题”文本框中，可以键入 FTP 站点标题消息。在客户端连接到 FTP 服务器之前，该服务器将显示此消息，在默认情况下消息为空；在“欢迎”文本框中键入欢迎消息。在客户端连接到 FTP 服务器时，该服务器将显示此消息，在默认情况下消息为空；在“退出”文本框中键入退出消息，在客户端注销 FTP 服务器时，该服务器将显示此消息，在默认情况下消息为空。

在“最大连接数”文本框中键入最大连接数消息。在客户端试图连接到 FTP 服务器，但由于 FTP 服务已达到允许的最大客户端连接数而失败时，该服务器显示此消息，在默认情况下消息为空。

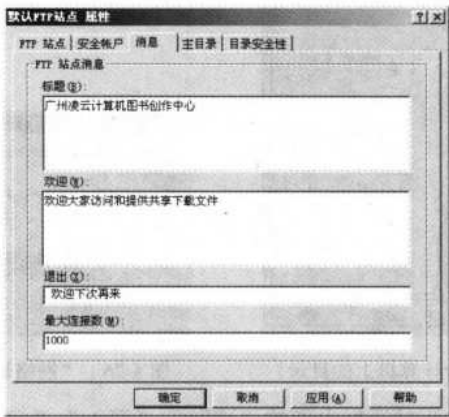


图 4-27 “默认 FTP 站点”属性对话框“消息”选项卡

(5) 以上 3 个选项卡的相应选项全部配置好以后，单击【确定】按钮退出，此时 FTP 站点的相应标识也将发生改变（在修改了“描述”的情况下），如图 4-28 所示。

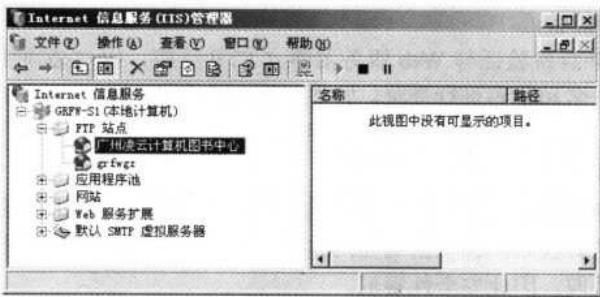


图 4-28 重新配置属性后的 FTP 站点

在创建了 FTP 站点后在右边的详细信息窗口中，并没有显示对应 FTP 主目录中的文件和文件夹，此时只需要在相应的 FTP 站点上单击鼠标右键，在弹出的快捷菜单中选择【资源管理器】命令，主目录中的所有文件和文件夹就会在右边的详细信息窗口中显示了，如图 4-29 所示。



图 4-29 显示了主目录中的文件和文件夹后的 FTP 站点

4.5 FTP 站点安全配置

FTP 站点的安全特性从底层同样受 IIS 结构、隔离模式和访问控制原理的影响，这方面在本书的第 2 章已有详细介绍，在此不再赘述。本章仅就 IIS 中 FTP 站点本身的安全配置方法进行介绍。在此主要介绍 FTP 站点的身份验证方式。

FTP 站点支持以下两种身份验证方法。

1) 匿名 FTP 身份验证

可以配置 FTP 服务器以允许对 FTP 资源进行匿名访问。如果为资源选择了匿名 FTP 身份验证，则接受对该资源的所有请求，并且不提示用户输入用户名或密码。这是可能的，因为 IIS 将自动创建名为 IUSR_computername 的 Windows 用户账户，其中 computername 是正在运行 IIS 的服务器的名称。这和基于 Web 的匿名身份验证非常相似。如果启用了匿名 FTP 身份验证，则 IIS 始终先使用该验证方法，即使已经启用了基本 FTP 身份验证，也是如此。

该验证方法不需要验证的用户凭据，最适于给不需要安全验证的信息授予公用访问权限。

摘要式身份验证和集成 Windows 身份验证无法用于 FTP 站点。必须在站点级别给 FTP 站点设置可用的验证设置。

2) 基本 FTP 身份验证

要使用基本 FTP 身份验证与 Web 服务器建立 FTP 连接，用户必须使用与有效 Windows 用户账户对应的用户名和密码进行登录。如果 FTP 服务器不能证实用户的身份，服务器就会返回一条错误消息。基本 FTP 身份验证只提供很低的安全性能，因为用户以不加密的形式在网络上传输用户名和密码。

该验证方法要求提供用户名和密码，提供低级别的安全性，最适于给需要很少或不需要保密性的信息授予访问权限。由于密码在网络上是以明文（未加密的文本）的形式发送的，这些密码很容易被截取，因此安全性很低。

下面是具体的配置方法。

(1) 在需要配置安全设置的 FTP 站点上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“安全账户”选项卡，如图 4-30 所示。

在这个选项卡中可以指定该 FTP 站点是否允许用户匿名登录。通常对外服务的 FTP 站点都允许匿名登录。如果允许的话，则需要选择“允许匿名连接”复选项，然后在下面配置一个用于匿名连接的用户账户（一定要是当前网络系统，或本地主机上合法、有效的账户）。系统已默认了一个匿名访问的账户“IUSR_服务器名”，密码也是系统自定的，我们无法知道，当然管理员可以在“Active Directory 用户和计算机”管理单元中的“Users”容器中找到这个用户（如图 4-31 所示），然后单击鼠标右键，在弹出的快捷菜单中选择【重设密码】命令修改密码即可。

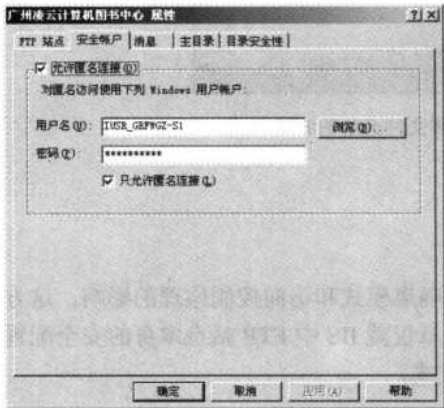


图 4-30 FTP 站点属性对话框“安全账户”选项卡



图 4-31 选择“IUSR_GRFWGWZ-S1”用户

要更改另一个已知权限和密码的其他账户，则可直接在“用户名”文本框中输入，或者通过单击【浏览】按钮，打开如图 4-32 所示的对话框中查找。然后在下面的“密码”文本框中输入相应账户的密码。在如图 4-30 所示的对话框中单击【应用】或【确定】按钮后会弹出如图 4-33 所示的密码确认对话框。重新输入指定用于匿名访问的用户账户密码，再单击【确定】按钮后生效。因为这里所配置的账户是用于所有匿名访问的用户访问 FTP 站点，所以应该只具有最低的权限。这样，所有以匿名访问的用户在访问 FTP 站点时，只需在打开的如图 4-34 所示的对话框中选择“匿名登录”复选项，然后单击【确定】按钮即可通过使用预定义的用户名和密码来匿名连接到 FTP 站点。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

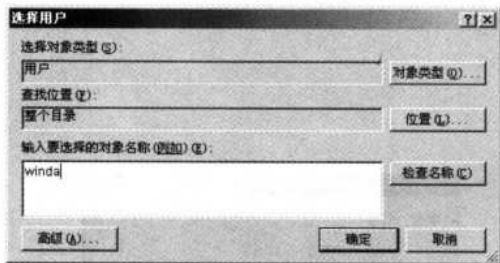


图 4-32 “选择用户”对话框

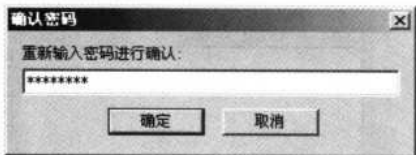


图 4-33 “确认密码”对话框

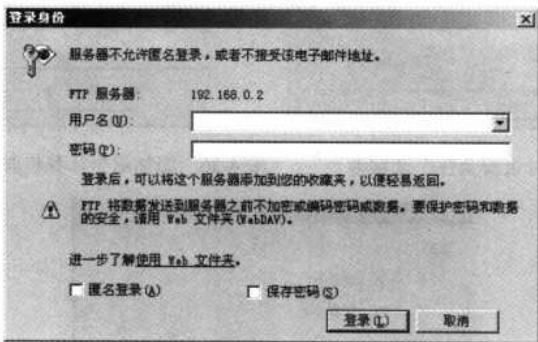


图 4-34 “登录身份”对话框



如果要允许一些特殊用户以高权限访问 FTP 站点，则一定不要选择“只允许匿名连接”复选项，否则在如图 4-31 所示的对话框中不能通过输入高权限用户账户来登录 FTP 站点，而只能以匿名账户访问了，这样也就无法使用高的权限。如果仅允许非匿名访问，则在如图 4-30 所示的对话框中一定要清除“允许匿名连接”复选项的选择，否则没有登录安全凭据的用户还是可以通过内置的匿名账户登录。

(2) 在如图 4-30 所示的对话框中选择“目录安全性”选项卡，打开如图 4-35 所示的对话框。这一点与第 1 章介绍的 Web 站点的“IP 地址与域名限制”选项配置类似。使用此选项卡可允许或阻止单个计算机或计算机组访问 FTP 站点。

在“TCP/IP 地址访问限制”栏中通过将计算机的 TCP 或 IP 地址指定为授权或拒绝访问权限，可以控制对 FTP 资源的访问，例如，站点、虚拟目录或文件。如果选择“拒绝访问”单选项，则可以拒绝所有计算机访问权限。要添加拒绝访问的计算机、计算机组或域，请单击【添加】按钮，打开如图 4-36 所示的对话框。在“拒绝访问”对话框中键入所需的信息。被拒绝访问的计算机将出现在如图 4-35 所示的对话框中的“下面列出的除外”文本框中。

如果选择“授权访问”单选项，则可以授予所有计算机访问权限。要添加允许访问的计算机、计算机组或域，请单击【添加】按钮，打开如图 4-37 所示类似的对话框。在“授权访问”对话框中键入所需的信息。授权访问的计算机同样会出现在如图 4-35 所示的对话框中的“下面列出的除外”文本框中。

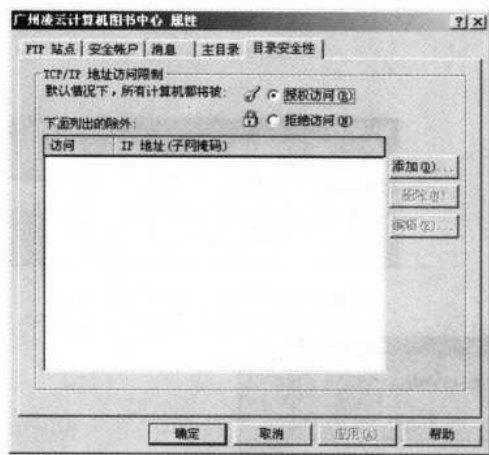


图 4-35 “目录安全性”选项卡

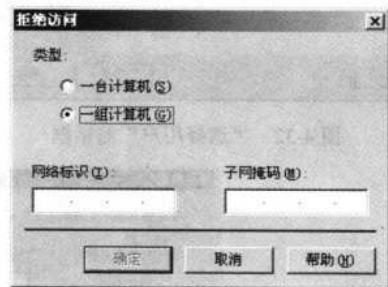


图 4-36 添加单个计算机时的“拒绝访问”对话框

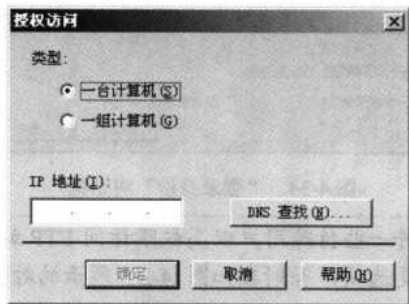


图 4-37 添加单个计算机时的“授权访问”对话框

通常来说，如果要拒绝或允许某些少数计算机的访问，则只需在图 4-36 或图 4-37 所示的对话框中选择“一台计算机”单选项，然后输入具体的计算机 IP 地址即可。如果拒绝或允许的是一组计算机，则要在图 4-36 或图 4-37 所示的对话框中选择“一组计算机”单选项，此时对话框对应变成如图 4-38 和图 4-39 所示了。此时需要配置这一组计算机的网络 ID 和子网掩码。这里的“网络标识”栏同样需要输入一个完整的网络 IP 地址，具体的 IP 地址范围是通过后面的“子网掩码”来确定的。具体参见第 2 章 2.6.4 节相对应的配置说明。

(3) 以上各项配置好后即可单击【确定】按钮完成，这样，以上所有设置即将生效。最后，如果要配置用户的非匿名访问权限，如 FTP 管理员、操作员等，则还需通过对 FTP 站点主目录，或者下面的子目录的 NTFS 访问权限配置来实现。这样也可以确保不同用户可以访问不同的目录，实现用户隔离。配置方法同样是在相应的 FTP 站点上单击鼠标右键，在弹出的快捷菜单中选择【权限】命令，打开如图 4-40 所示的对话框。对需要较高权限的用户或组账户配置较高的访问权限，对不需要特别权限的用户或组账户，从权限列表中删除。当然，也可以在资源管理器中，找到相应的 FTP 站点目录，单击鼠标右键，在弹出的快捷菜单中选择【共享与安全】命令，在打开的对话框中配置。实际上就是 NTFS 文件夹或文件的安全访问权限配置，这就是之所以把 Web 和 FTP 站点主目录放在 NTFS 格式磁盘分区的原因。具体配置方法参见本系列丛书的《网管员必读——网络管理》一书，在此不再赘述。

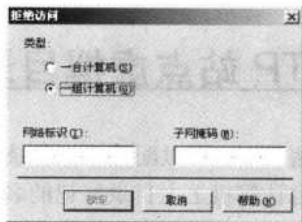


图 4-38 添加一组计算机时的“拒绝访问”对话框

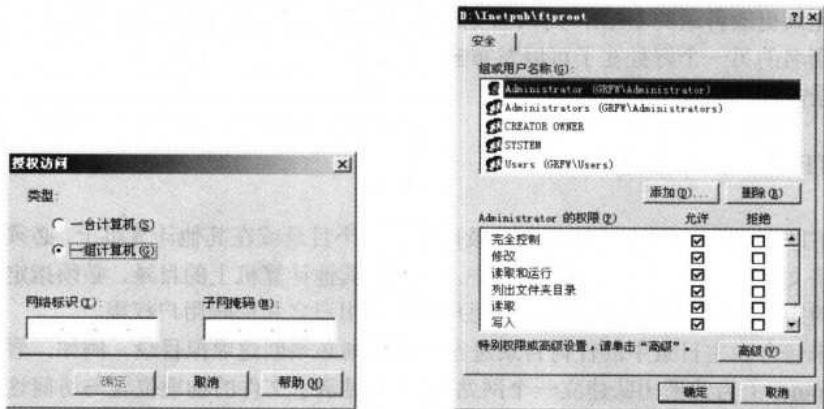


图 4-39 添加一组计算机时的“授权访问”对话框 图 4-40 FTP 站点主目录“安全”选项卡



FTP 站点所支持身份验证方式很简单，只有两种：匿名身份验证和基本身份验证，不支持摘要式身份验证和集成 Windows 身份验证。而且所支持的基本身份验证方式采用的是明文密码传送方式，存在较大安全隐患，特别是在对外的 FTP 站点中。FTP 站点也不支持数据加密。要保护密码和数据加密，则需要采用 Web 文件夹（WebDAV）。

WebDAV 与文件传输协议（FTP）相似，但是，WebDAV 可以为通过 Web 进行文件传输提供更安全的环境。在 WebDAV 中需要使用安全套接字层（SSL）来进行安全访问。

当将信息发送到运行 SSL 的 Web 服务器时，WebDAV 将保护密码和所加密的数据。如果服务器没有运行 SSL，那么若将服务器配置为使用 Windows 身份验证，WebDAV 就可以保护密码。然而，不能对发送到服务器的数据进行加密。如果服务器运行 SSL，则服务器的 Internet 地址将以 https://开始，而不是 http://开始。

登录到服务器时，FTP 不使用加密或其他安全机制来保护密码。此外，在使用 FTP 将文件发送到服务器或从服务器上获取文件时，不能对数据进行加密。这种情况将使信息处于危险状态，因为传输信息时，使用网络硬件或软件的任何人都能截获该信息。

使用 WebDAV 将文件、文件夹和其他数据传输到运行 SSL 的 Web 服务器是传输信息的最安全方法。

4.6 创建和配置 FTP 站点虚拟目录

与 Web 站点一样，在 FTP 站点中也可以配置虚拟目录。FTP 站点的虚拟目录就是不在 FTP 主目录下的物理目录或另一台计算机上主目录好记的名称或别名。由于别名通常要比物理目录的路径名短，更便于用户输入。使用别名也很安全，因为用户不知道文件在服务器上的物理位置，所以，便无法使用这些信息来修改文件。使用别名也可以更方便地移动站点中的目录，无须更改目录的 URL，而只需更改别名与目录物理位置之间的映射。

使用别名的另一个好处在于可以发布多个目录下的内容以供所有用户访问，单独控制每个虚拟目录的读/写权限。

4.6.1 FTP 虚拟目录概述

如果 FTP 站点包含的文件位于主目录以外的某个目录或在其他计算机上，必须创建虚拟目录将这些文件包含到自己的 FTP 站点中。要使用其他计算机上的目录，必须指定该目录的通用命名约定（UNC）名称并提供验证用户权限的用户名和密码用户权限。

要从未包含在主目录中的任何目录进行发布，则必须创建虚拟目录。例如，假定你要在公司的 Intranet 上为营销团队建立一个网站。表 4-1 显示了文件的物理位置与访问这些文件的 URL 之间的映射关系。

表 4-1 虚拟目录所在物理位置与 URL 之间的关系

物理位置	别名	URL
C:\inetpub\ftproot	主目录（无）	ftp://SampleFTPSite
\\Server2\SalesData	Customers	ftp://SampleWebSite/Customers
D:\Marketing\PublicRel	PR	ftp://SampleFTPSite/PR

虚拟目录和物理目录（不带别名的目录）都显示在 IIS 管理器中。图 4-41 显示了上述的 FTP 站点示例，其中 Customers 和 PR 均为虚拟目录。

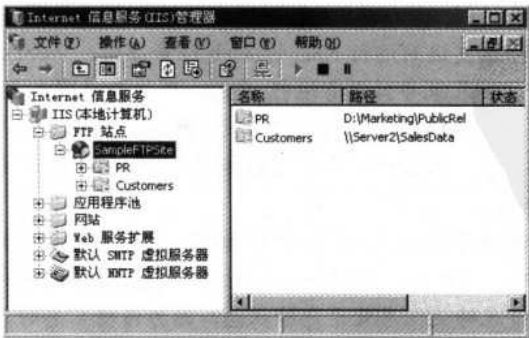


图 4-41 FTP 站点的虚拟目录

对于一个初级 FTP 站点，通常不需要添加虚拟目录。只需将所有文件放在该站点的主目

录中即可。如果站点比较复杂，或者需要为站点的不同部分指定不同的 URL，则可以根据需要添加虚拟目录。要从多个站点访问某个虚拟目录，必须为每个站点添加虚拟目录。

对于匿名用户，必须将虚拟目录映射到在工作文件夹下，为匿名用户专门创建的文件夹上，例如，C:\inetpub\ftproot\localuser\public。如果要为使用用户隔离的站点设置虚拟目录，可以设置每用户虚拟目录，因为所有的用户都被隔离于自己的工作目录中。例如，如果 USER1 的工作文件夹为 C:\inetpub\ftpRoot\localuser\USER1，你希望 USER1 访问你创建的虚拟目录，则虚拟目录应映射到上述路径中的文件夹上。在这种情况下，其他用户均无法访问该虚拟目录，除非他和 USER1 使用相同的工作目录。

如果要为站点设置使用 Active Directory 目录服务的用户隔离虚拟目录，并且 USER1 的工作文件夹映射到 \\computer\User1Share 上，那么，必须创建映射到该路径下文件夹的虚拟目录，在这种情况下，只有将工作文件夹映射到上述路径的用户才能访问虚拟目录。

4.6.2 创建和删除 FTP 站点虚拟目录

如下是两种创建或删除虚拟目录的方法。

- 使用 IIS 管理器。
- 使用 iisftpr.vbs 管理脚本。

当然，你必须是本地计算机上 Administrators 组的成员或者必须被委派了相应的权限，才能执行下列步骤。作为安全性的最佳操作，请使用不属于 Administrators 组的账户登录计算机，然后使用运行方式命令以管理员身份运行 IIS 管理器。

1. 使用 IIS 管理器创建虚拟目录

(1) 在 IIS 管理器中，展开本地计算机，展开“FTP 站点”文件夹，展开要添加虚拟目录的 FTP 站点，在要创建虚拟目录的站点或文件夹上单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【虚拟目录】命令，打开如图 4-42 所示的对话框。

(2) 单击【下一步】按钮，打开如图 4-43 所示的对话框。在“别名”文本框中键入虚拟目录的名称。这是用户键入的名称，也就是虚拟目录的别名，应该简短且易于键入。

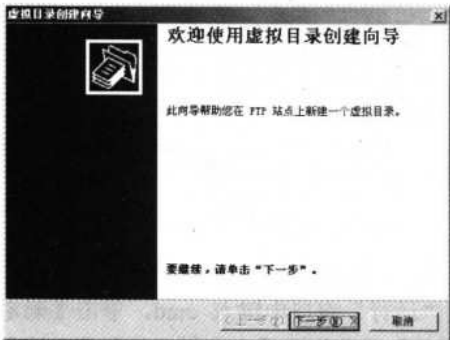


图 4-42 “欢迎使用虚拟目录创建向导”对话框

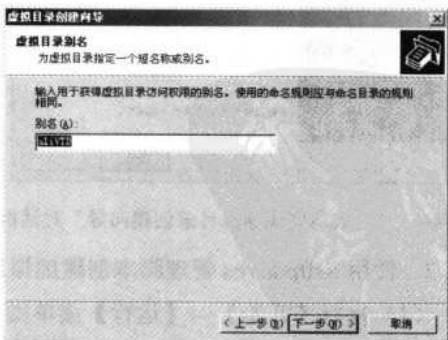


图 4-43 “虚拟目录别名”对话框

在这里输入的虚拟目录别名要考虑这个目录的访问对象范围，如果 FTP 站点中采用了隔离方式，且相应的虚拟目录是只针对某个用户或者组用户访问的，则所取的虚拟目录别名最

好有一定的象征性，这样便于管理。如为用户 Alice 配置的虚拟目录，则可以为虚拟目录取名为“aliVTD”（代表 Alice 用户的虚拟目录）。

(3) 单击【下一步】按钮，打开如图 4-44 所示的对话框。在“路径”文本框中键入，或浏览到虚拟目录所在的物理目录，也就是实际路径。这个目录不应是在相应 FTP 站点主目录下。

(4) 单击【下一步】按钮，打开如图 4-45 所示的对话框。在“允许下列权限”栏下面，选择所需访问权限复选项。如果选择“读取”（浏览和下载）复选项，则除非另外配置，用户访问的权限均限于读取权限；如果同时选择了“写入”（上传）复选项，则除非另外配置，用户访问的权限可同时具有读取和写入权限。当然，如果仅选择“写入”复选项，则除非另外配置，用户只允许把文件上传到该虚拟目录中。

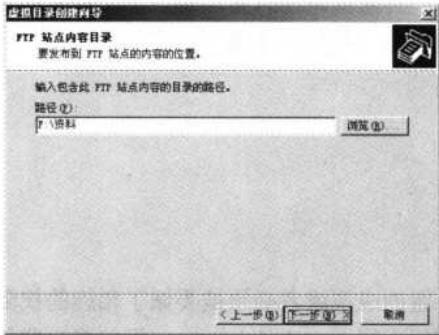


图 4-44 “FTP 站点内容目录”对话框

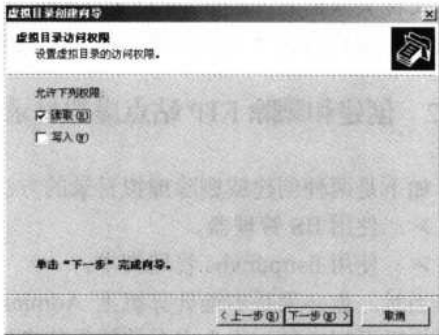


图 4-45 “虚拟目录访问权限”对话框

(5) 单击【下一步】按钮，打开如图 4-46 所示的对话框。单击【完成】按钮，完成虚拟目录在当前选定的文件夹级别下创建。创建了的虚拟目录如图 4-47 所示。



图 4-46 “已成功完成虚拟目录创建向导”对话框

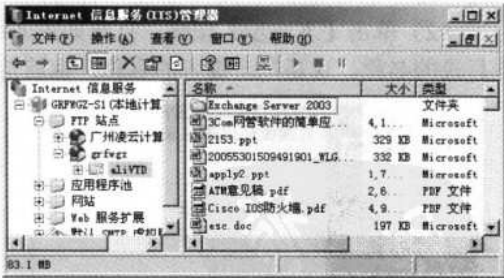


图 4-47 新创建的 FTP 站点虚拟目录

2. 使用 iisftpr.vbs 管理脚本创建虚拟目录

(1) 执行【开始】→【运行】菜单操作，在“运行”窗口中键入 cmd，单击【确定】按钮进入命令提示符窗口（当然也可以直接从【附件】菜单执行【命令提示符】菜单进入）。

(2) 利用 CD 命令进入到相应系统目录下的 system32 文件夹（如果配置了路径变量则不必，可在任何路径下操作）。在命令提示符下键入 cscript iisftpr.vbs /create “SampleFTPSite”（在此处输入实际的 FTP 站点名）VirtualDirectoryName（在此输入虚拟目录别名）x:\path（在

此输入虚拟目录实际物理路径)，并按回车键。

通过以上两步就完成了虚拟目录的创建，系统会有相应的提示，如图 4-48 所示。



图 4-48 利用 iisftpr.vbs 脚本创建虚拟目录的示例

再回到 IIS 管理器中，找到相应的 FTP 站点或文件夹下，即可见到刚才利用 iisftpr.vbs 脚本创建的虚拟目录了，如图 4-49 所示。

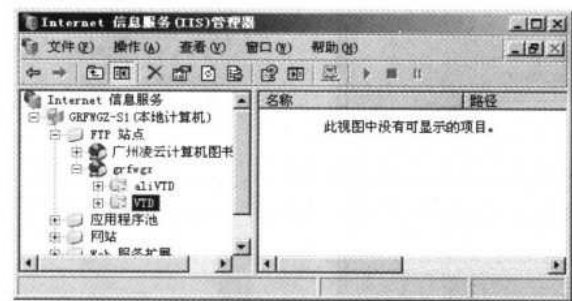


图 4-49 利用 iisftpr.vbs 脚本创建的虚拟目录

3. 删除虚拟目录

与虚拟目录的创建一样，删除虚拟目录也有两种方法：IIS 管理器法和 iisftpr.vbs 脚本法。下面分别予以简单介绍。



注意

删除虚拟目录操作不会删除相应的物理目录或文件。

1) 使用 IIS 管理器删除虚拟目录

在 IIS 管理器中删除虚拟目录的方法很简单，只需在 IIS 管理器中，展开包含要删除虚拟目录的 FTP 站点或文件夹，在该虚拟目录上单击鼠标右键，在弹出的快捷菜单中选择【删除】命令，然后在提示框中单击【是】按钮即可完成。

2) 使用 iisftpr.vbs 管理脚本删除虚拟目录

此方法不适用于根虚拟目录的删除。方法是在命令提示符下运行如下命令：`cscript iisftpr.vbs /delete "SampleFTPSite"`（要删除虚拟目录的 FTP 站点）`VirtualDirectoryName`（虚拟目录别名），然后按回车键即可完成删除。

4.6.3 虚拟目录的配置

虚拟目录与 FTP 站点一样，也具有一些独立的属性配置。如它也可以配置成只允许个别

用户或组用户访问，使它成为用户的主目录，实现与其他用户的主目录隔离。还可以配置允许或授权访问的 IP 地址计算机。下面是具体的介绍。

(1) 在相应的虚拟目录上单击鼠标右键，在弹出的快捷菜单中选择“属性”选项，打开如图 4-50 所示的对话框。在这时可以重新配置虚拟目录的物理位置和用户访问权限选项。

如果要改变该虚拟目录的物理位置，则可在“此资源的内容来源”栏中选择相应选项，然后配置相应的位置。这一点与前面介绍的 FTP 站点属性配置中的图 4-24 一样，参见 4.4 节相关内容即可。

在这里也可以为该虚拟目录配置普通用户的访问权限。系统默认是选择了“读取”和“记录访问”两个复选项，“读取”选项是配置用户允许读取（如浏览和下载），“记录访问”是针对日志记录的，选择后系统只记录用户对该目录的访问。

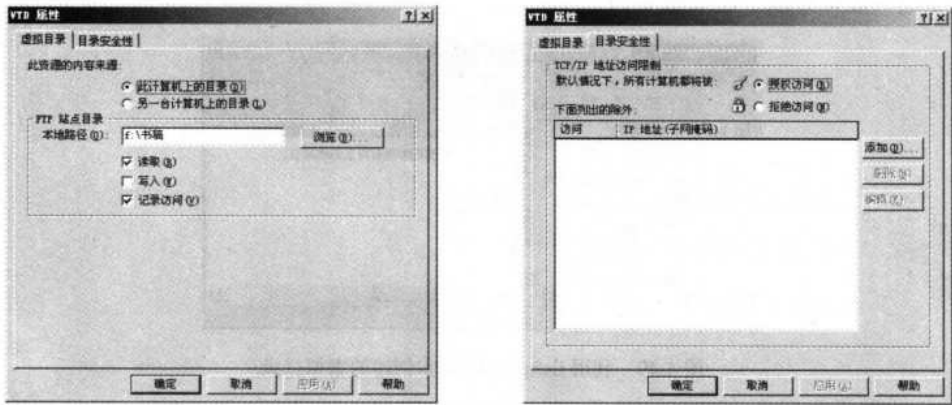


图 4-50 虚拟目录属性对话框“虚拟目录”选项卡 图 4-51 虚拟目录属性对话框“目录安全性”选项卡

(2) 在如图 4-24 所示的对话框中，选择“目录安全性”选项卡，打开如图 4-51 所示的对话框。这一对话框的配置方法与 4.5 节的图 4-35 所示的对话框是一样的，参见前面介绍的方法即可。

除了属性配置外，同样也可以为不同用户设置不同的 NTFS 安全访问权限。方法同样可以直接在相应的虚拟目录上单击鼠标右键，在弹出的快捷菜单中选择【权限】命令，在打开的“安全”选项卡对话框中配置，也可以在资源管理器中找到虚拟目录的物理目录，然后单击鼠标右键，在弹出的快捷菜单中选择【共享与安全】命令，在打开的“安全”选项卡对话框中配置即可。具体配置方法参见本系列丛书的《网管员必读——网络管理》一书。



因为 FTP 站点的管理非常简单，通常可直接在 IIS 管理器中进行即可（当然也可以用 iisftp.vbs 脚本执行命令），但一般的企业 FTP 管理很少用到。出于整部书的篇幅考虑，在此不作介绍。下面着重介绍功能更强大的 Serv-U FTP 站点方案。对于采用共享方式上网的用户，外网用户要访问 FTP 站点仍需要进行端口映射，如果没有固定外网 IP 地址，而是采用域名方式访问，则同样也要进行动态域名解析，具体内容参见本书的第 1 章介绍。

4.7 利用 Serv-U 组建 FTP 站点的基本思路

现在可以用来组建 FTP 服务器的软件很多，典型代表如 Serv-U、Leapwear 等。为了便于大家的理解，在此就以 Serv-U 的最新版本 6.3.0.1 的汉化版来介绍 FTP 站点的创建与配置方法。

Serv-U 是 Rob Beckers 开发的一个功能强大的、简单易用的、成熟的 FTP 服务器，FTP 服务器用户通过 Internet 的 FTP 协议共享文件，Serv-U 不仅仅能 100%适用于标准的 FTP，同样也包括了很多功能，是一个完美的文件共享解决方案。

FTP Serv-U 其他的安全功能如下。

- 用 SSL 加密数据。
- ODBC 的支持。
- 带宽限制。
- 目录和文件的权限管理。
- IP 限制。
- 用户的时时监控器。
- 用户的所有操作记录。
- 能为所有的，包括每一个人和每一个组定制安全设置。

要使用 Serv-U 建设的 FTP 站点能正常工作，通常需按如下基本思路进行各种设置。

1) Serv-U 程序的安装与 FTP 站点的创建

Serv-U 程序的安装与其他 Windows 平台程序一样，没有太大区别，只是在安装时需要稍稍注意一些事项。

利用 Serv-U 进行 FTP 站点的创建有两种不同的途经：一种是利用在程序安装后自动打开的 FTP 站点设置向导创建；另一种就是在任何需要新站点时利用新建 FTP 站点向导来创建。

具体步骤将在 4.8 节介绍。

2) 服务器和域全局设置

在 Serv-U 中，不仅可以对各 FTP 域进行全局设置，还有专门针对 FTP 服务器的全局设置选项，如上传、下载速率、连接用户、SSL 安全连接。

在各 FTP 域中，全局设置中也包括许多选项，如域虚拟目录、消息格式、IP 地址过滤和事件记录日志等。

具体设置方法参见 4.9 节。

3) 配置域用户和组账户选项

在 Serv-U 中，系统中的用户和组账户是由 Serv-U 程序自己管理的，不是 Windows 系统中的用户和组账户。在这些用户中，我们可以为他们各自配置多个不同的主目录、子目录及访问权限；每个用户所允许的最大上传、下载速率；每个用户的磁盘配额大小。对于组账户可以配置多个主目录和子目录，组织不同的用户成员。

具体配置方法参见 4.10 节。

4) 创建虚拟目录（可选）

在 Serv-U 中可在主目录之外（如网络中的其他计算机上）为站点和用户指定多个虚拟目

录，这样，访问时就像直接访问 FTP 服务器一样。

5) 动态域名解析和端口映射配置（可选）

动态域名解析也是针对没有固定外网 IP 地址的对外 FTP 站点而言的，如果 FTP 站点仅用于局域网内部，则无须配置；而端口映射则是针对 FTP 服务器没有直接连接互联网，而是通过其他途经共享上网的情况的。具体也请参见本书的第 1 章介绍。

4.8 Serv-U 的安装与 FTP 站点创建

程序的安装与站点的创建是 FTP 站点使用的两个基本前提。本节要向大家介绍，Serv-U 汉化程序的安装和 FTP 站点创建的两个基本方法。

4.8.1 Serv-U 的安装

程序安装没什么特别，与其他的 Windows 程序一样，只是在安装后会有一些选项需要确认、配置，否则后面创建的 FTP 站点，用户可能无法连接上。

汉化版的安装也必须在安装英文版的原程序后进行。在英文原程序安装后，如果系统中有防火墙（如 Windows 系统自带的 Windows 防火墙），则会弹出如图 4-52 所示的对话框，要求确认是否让 Serv-U 服务作为防火墙的例外程序，也就是让 Serv-U 程序通过，不阻挡。当然需要这样了，否则网络用户就无法连接到 FTP 站点。按系统默认，选择“Add Serv-U as an exception to the Windows Firewall”复选项，然后单击【Next】按钮，打开如图 4-53 所示的对话框。Serv-U 除了能自动检测并配置防火墙系统外，还可以自动检测并配置网络出/入口线路中的即插即用设备，如路由器，选择“Allow Serv-U to configure your UPnP capable router(s)”复选项。

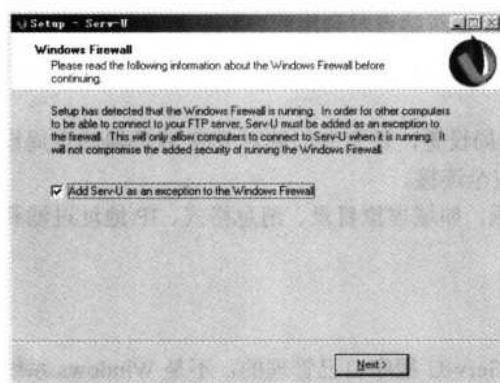


图 4-52 “Windows Firewall”对话框

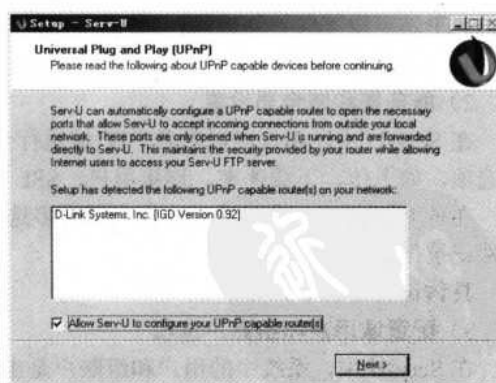


图 4-53 “Universal Plug and Play (UPnP)”对话框

利用 Serv-U 组建 FTP 站点，相对 IIS 来说要灵活许多，功能也要强大许多。它不仅可以创建自己的用户和主目录，还可以创建共享同一主目录的用户组，相当于 IIS 中的用户隔离。另外，在 Serv-U 中还可以为用户配置多个访问目录；配置上传/下载速率限制、所占用的带宽比例；配置用户连接数限制；配置磁盘配额（在 IIS FTP 站点也可以，但需要在系统

中配置)；配置高级 SSL 安全连接等。

英文原程序安装后，系统会自动打开第一个 FTP 站点创建向导，这将在下节具体介绍。第 1 个站点创建好后，就可以继续安装汉化程序来汉化原英文程序了。当然也可以在系统自动启动的如图 4-54 所示的向导首页中，单击【Cancel】按钮取消后面的第 1 个 FTP 站点创建过程，直接先安装汉化程序，这样，在创建向导中也将是中文界面，方便理解。但是建议不要取消系统自动打开的第 1 个 FTP 域创建向导，因为它与单纯的域创建向导存在较大的不同，在该过程中还有许多比较实用的配置选项。

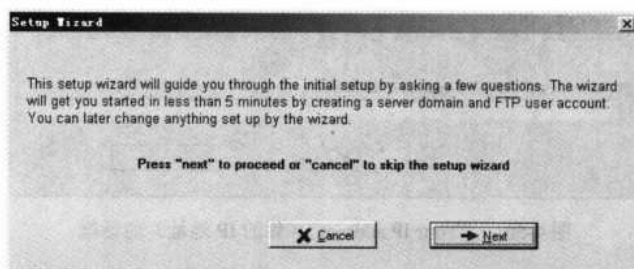


图 4-54 设置向导首页

4.8.2 利用设置向导创建第 1 个 FTP 站点

在英文原程序安装完成后，系统会立即启动一个 FTP 站点设置向导，利用这个向导可以创建第 1 个 FTP 站点。下面是具体的设置步骤。

(1) 在英文原程序安装，并关闭安装界面时，系统会自动打开如图 4-54 所示的向导界面。在此首页对话框中询问是否要立即进行站点设置向导，如果要立即运行向导，则单击【Next】按钮，向下进行；否则单击【Cancel】按钮，退出设置向导，在程序安装后待需要时再运行。在此，选择立即运行设置向导。

(2) 单击【Next】按钮，打开如图 4-55 所示的对话框。在这个对话框中询问是否要在开始菜单中添加小图标的 Serv-U 程序选项，这主要是为了美观界面，一般情况下没什么问题，但有些配置比较低的计算机上可能不能完全显示这些图标。如果确认自己所用系统显示小图标没问题选择“**Yes**”单选项，在开始菜单中添加带有小图标的程序选项。如果选择“**No**”单选项，则在开始菜单中仅显示程序选项的文字标题。

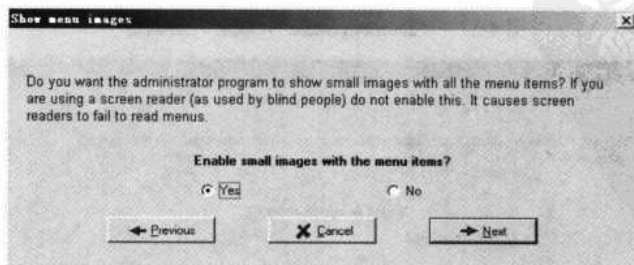


图 4-55 “Show menu images”（显示菜单图标）对话框

(3) 单击【Next】按钮，打开如图 4-56 所示的对话框。在这里要输入你的 FTP 服务器

212 网管员必读——网络应用（第2版）

IP 地址，如果你的 FTP 服务器是直接连接互联网的，而且有固定的 IP 地址，则可直接输入互联网 IP 地址；而如果采用的是拨号等动态 IP 分配方式上网，没有固定外网 IP 地址，则不用在这里输入 IP 地址。如果 FTP 服务器是通过共享方式上网，且有固定局域网 IP 地址，则在此输入 FTP 服务器的静态局域网 IP 地址；如果是采用动态局域网 IP 地址，则在此也不用输入。这里以不输入 FTP 服务器 IP 地址为例进行介绍。

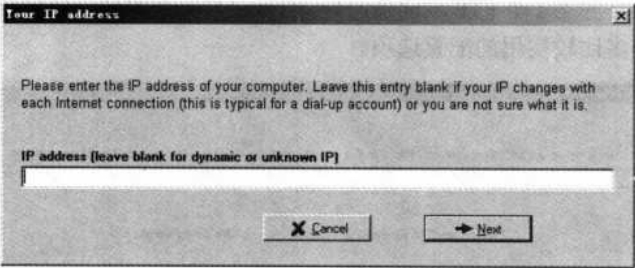


图 4-56 “Your IP address”（你的 IP 地址）对话框

（4）单击【Next】按钮，打开如图 4-57 所示的对话框。在这里要给 FTP 站点输入一个域名的描述。如果 FTP 站点是放在互联网上的，则必须有一个唯一的互联网域名（需事先申请），然后可在这里输入类似如 ftp.domain.com 之类的域名描述，这是用来标识相应 FTP 站点的。如果 FTP 站点仅是在局域网内部运行，则可不需要互联网域名，可随便指定一个 FTP 服务器域名的描述即可。

（5）单击【Next】按钮，打开如图 4-58 所示的对话框。在这里询问是否要把所设置的 FTP 服务器当做系统的一个服务，随计算机的启动而启动？如果需要这样，则选择“Yes”单选项，否则选择“No”单选项。

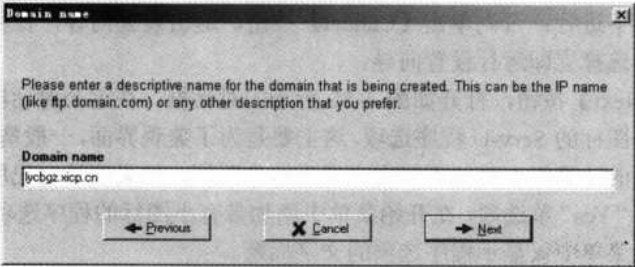


图 4-57 “Domain name”（域名）对话框

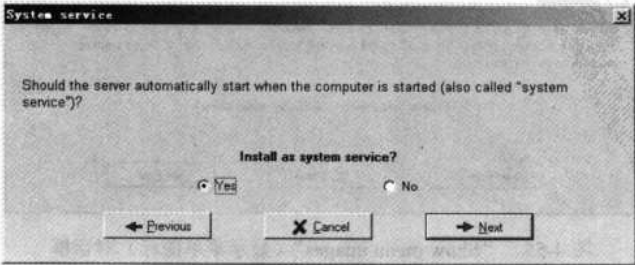


图 4-58 “System service”（系统服务）对话框

(6) 单击【Next】按钮，打开如图 4-59 所示的对话框。在这里询问是否需要允许匿名访问 FTP 站点。如果允许则选择“**Yes**”单选项，否则选择“**No**”单选项。一般来说需要允许匿名访问，特别是放在互联网上的 FTP 站点。在此以允许匿名访问为例进行介绍。

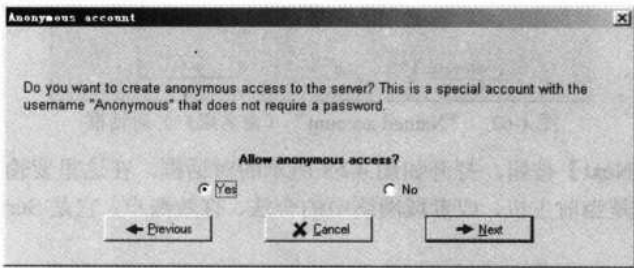


图 4-59 “Anonymous account”（匿名账户）对话框

(7) 单击【Next】按钮，打开如图 4-60 所示的对话框。在这里要为匿名访问用户指定一个允许访问的站点主目录，指定后，在匿名用户登录 FTP 站点后直接进入这个主目录。

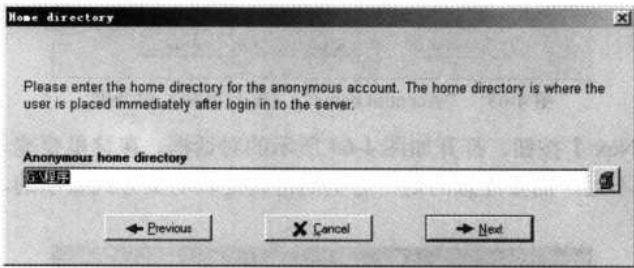


图 4-60 “Home directory”（主目录）对话框

(8) 单击【Next】按钮，打开如图 4-61 所示的对话框。在这里询问是否要把匿名用户的访问锁定在上一步指定的主目录上。这样一来匿名用户就只能访问上一步指定的主目录下的文件，而不能访问其他目录下的文件。如果是，则选择“**Yes**”单选项，否则就选择“**No**”单选项。一般来说对于普通的匿名用户来说锁定是需要的，这是出于 FTP 服务器安全考虑的。

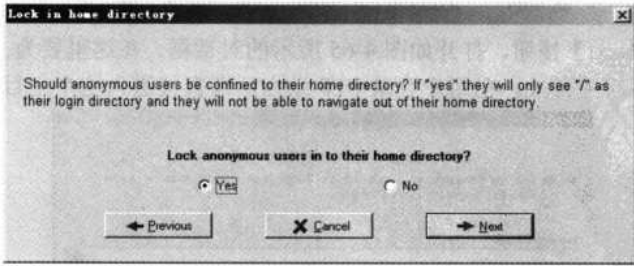


图 4-61 “Lock in home directory”（锁定在主目录中）对话框

(9) 单击【Next】按钮，打开如图 4-62 所示的对话框。在这里询问是否要为 FTP 站点创建一个新的账户，这个账户需要用账户名和密码来登录。这通常是为有特殊权限需要的人配置的，如站点操作员和站点管理员，当然也可以在此不创建，因为系统管理员总是有权限创建各种权限的用户的，可以随时创建。在此以选择“**Yes**”单选项为例进行介绍。

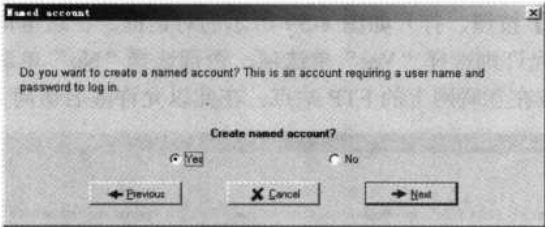


图 4-62 “Named account”（命名账户）对话框

（10）单击【Next】按钮，打开如图 4-63 所示的对话框。在这里要输入新建账户名称，这个账户名不要求是当前主机，或者域网络中的合法、有效账户。它是 Serv-U 自己的账户系统中的用户。

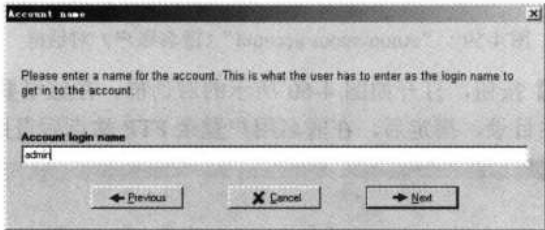


图 4-63 “Account name”（账户名称）对话框

（11）单击【Next】按钮，打开如图 4-64 所示的对话框。在这里要输入上一步指定的账户所对应的密码。不过，需要注意的是，这里的密码是以明文方式显示的，一定要注意不要让其他人看到。

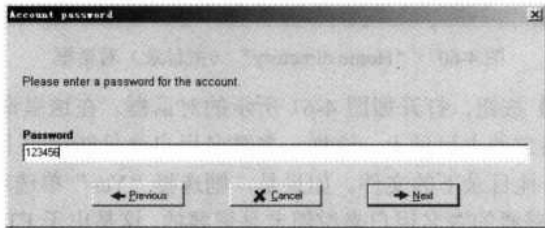


图 4-64 “Account password”（账户密码）对话框

（12）单击【Next】按钮，打开如图 4-65 所示的对话框。在这里要为上述指定的账户配置一个 FTP 站点访问主目录。在用户登录 FTP 站点后即直接进入这个主目录。

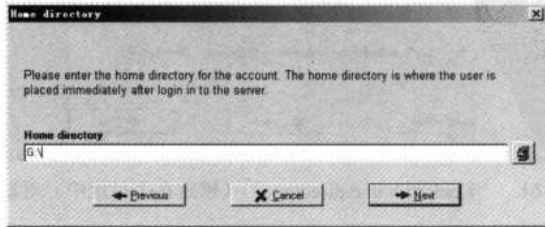


图 4-65 “Home directory”（主目录）对话框

（13）单击【Next】按钮，打开如图 4-66 所示的对话框。在这里询问是否要把上述账户的访问范围锁定在上一步指定的主目录中。一般来说，对于操作员和管理员则不用锁定，选

择 “No” 单选项，不锁定。

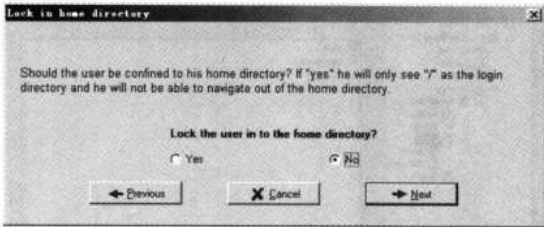


图 4-66 “Lock in home directory”（锁定在主目录中）对话框

(14) 单击【Next】按钮，打开如图 4-67 所示的对话框。在这里要选择上述配置的用户是否要具有管理权限，具体要根据所指派的账户类型而定。如果是为操作员，或者管理员配置的，则在此要指派相应的管理权限，否则无法担当相应职责。在这里有 5 个可选项：如果选择 “No Privilege”（无特权）选项，则所指派的账户不具有特殊的管理权限，但仍可以具有基本的管理权限，可用远程管理；如果选择的是 “Group Administrator” 选项，则它为组管理员权限，具有远程管理组账户权限，包括查看组成员和新建组用户账户；如果选择的是 “Domain Administrator” 选项，则它为相应域的管理员权限，可以管理、新建域中用户和组账户，修改域设置，当然也可以用于 FTP 域的远程管理；如果选择的是 “System Administrator” 选项，则它具有管理整个 FTP 系统的权限，权限最高，所具有的权限包括 Serv-U 程序中服务器和所有域的设置更改、新域、用户和组的创建等，不受任何限制；如果选择的是 “Read-Only Administrator” 选项，则它具有只读权限的管理权限，仅能查看当前的服务器和域设置，不能更改任何已有设置。

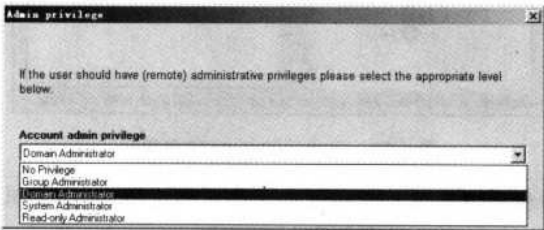


图 4-67 “Admin privilege”（管理特权）对话框

(15) 单击【Next】按钮，打开如图 4-68 所示的对话框。在这里提示向导即将完成，单击【Finish】按钮完成向导。完成后即可在 Serv - U 主界面中见到刚才所创建的 FTP 站点，如图 4-69 所示。从 Serv-U 主界面中可以看到，刚才新建的匿名访问用户 Anonymous 和域管理员 admin 账户。

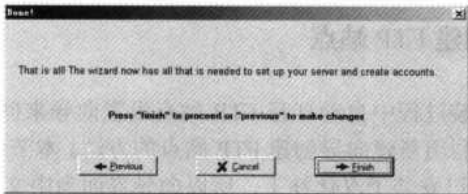


图 4-68 “Done!”（完成）对话框

216 网管员必读——网络应用（第2版）

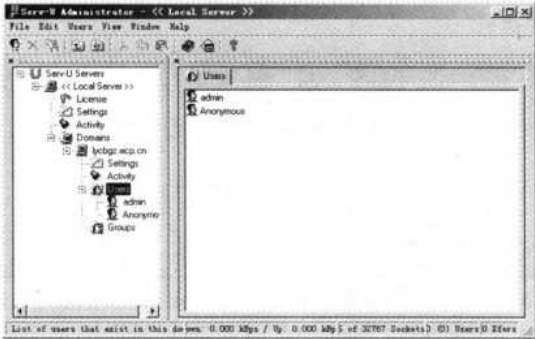


图 4-69 新创建的 FTP 站点

随后可以安装汉化程序补丁了，汉化后的 Serv-U 界面如图 4-70 所示。现在的汉化补丁通常只是汉化界面、菜单和工具栏，并没有汉化帮助系统，所以在需要帮助时仍能查看英文帮助。



图 4-70 汉化后的 Serv-U 主界面



注意

利用程序安装时打开的设置向导所创建的 FTP 域只能是采用由自己管理的用户系统，而不能创建直接采用 Windows 工程 NT 域用户系统（这一点将在下节具体介绍），所以在创建后的 FTP 域中包括了“用户”和“组”两个功能项，参见图 4-70。而且，在这样的一个自管理用户系统的 FTP 域中，可以创建用于匿名访问的用户账户，也就是允许匿名连接相应的 FTP 域站点；而采用 Windows 工程 NT 域用户系统的 FTP 域不能配置匿名账户，也就无法采用匿名方式访问对应的 FTP 域站点了。

4.8.3 利用新建向导创建 FTP 站点

上节是利用程序在安装过程中自动打开 FTP 站点设置向导来创建的第 1 个 FTP 站点，本节要介绍的是在需要时利用新建向导创建 FTP 站点的方法。本节所创建的是一个用于局域网的 FTP 站点。因为此时已安装了汉化补丁，所以向导界面为中文，更加容易理解。

（1）在如图 4-70 所示的主界面左边导航栏的“域”节点上，单击鼠标右键，在弹出的

快捷菜单中选择【新建域】命令，打开如图 4-71 所示的对话框。在这里可为新 FTP 站点域指定一个 IP 地址，同样也可不指定，不指定的话，则当前服务器系统网卡上可用的所有没有被其他站点使用的 IP 地址均适用于此站点。因为所要创建的是一个仅用于局域网的 FTP 站点，所以可以在此配置一个静态的局域网 IP 地址。

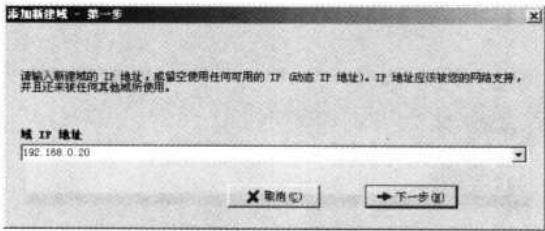


图 4-71 “添加新建域—第一步”对话框

(2) 单击【下一步】按钮，打开如图 4-72 所示的对话框。在此要指定新建 FTP 站点的域名，如果仅用于局域网，则可随便指定一个，在此，以当前 NT 域网络的域名为例。

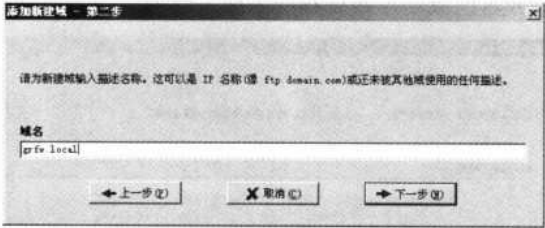


图 4-72 “添加新建域—第二步”对话框

(3) 单击【下一步】按钮，打开如图 4-73 所示的对话框。在此要指定新建的 FTP 站点所用的端口，默认均为 FTP 服务的 21 号端口，也可以更改，但一定要告知用户，以便访问时加上修改后的端口（采用默认端口，在访问时不用指定端口号）。因为属于局域网的 FTP 站点，为了不与其他 FTP 站点的端口相冲突，在此选择了另外一个端口，只要在 1~65 535 之间都可以，但最好是在 1 024 以后的端口，因为前面的端口为常见端口，通常已指派给了其他服务。

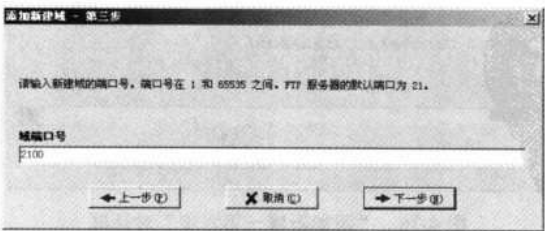


图 4-73 “添加新建域—第三步”对话框

(4) 单击【下一步】按钮，打开如图 4-74 所示的对话框。在这里要选择域类型，通常对于比较小的域，则选择“存储于.INI 文件”选项，而对于大的域，则可选择“存储于计算机注册表”选项，这两种域类型中用户账户都是由 Serv-U 程序自己管理的，如果选择了“存

218 网管员必读——网络应用（第2版）

储于 ODBC 数据库中”选项，则用户账户直接采用数据库系统中的用户账户系统。还可以选择“使用 Windows NT-SAM/AD 用户账号”选项，直接采用 Windows NT 系统的用户账户。在此，因为所创建的 FTP 站点是用于局域网用户访问，所以为了方便和安全起见，选择采用 Windows NT 域账户类型。

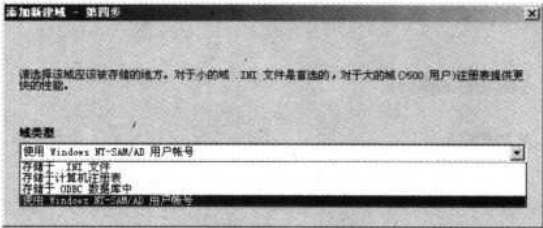


图 4-74 “添加新建域—第四步”对话框

(5) 选择了“使用 Windows NT-SAM/AD 用户账号”选项后，单击【下一步】按钮，即打开如图 4-75 所示的对话框。在这里要求指定所在的 Windows 域名，直接输入当前域名即可，但要确保 FTP 服务器已成功连接到相应的域网络中。

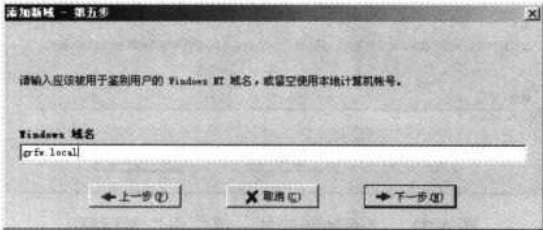


图 4-75 “添加新建域—第五步”对话框

(6) 单击【下一步】按钮，打开如图 4-76 所示的对话框。在这里要为 FTP 站点指定一个主目录，以供域系统中所有用户连接 FTP 站点时直接进入。因为此处选择的是直接利用 Windows NT 域中的用户账户，所以不能为每个用户配置不同的主目录，所以域用户共享一个主目录，当然，仍可以配置多个虚拟目录，具体内容将在本章后面介绍。

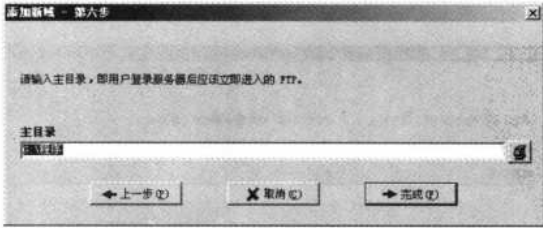


图 4-76 “添加新建域—第六步”对话框

(7) 单击【完成】按钮，完成新 FTP 站点的创建过程。新建的站点都会在“域”节点下显示。因为本节所创建的站点采用的是 Windows NT 域中的账户系统，所以没有“用户”和“组”两个节点，如图 4-77 所示。



图 4-77 新建的 FTP 站点

4.9 服务器与域全局设置

在 4.7 节就介绍到，这里所说的全局设置包括两方面：Serv-U 服务器设置和 FTP 域设置。服务器设置同时作用于程序中的所有 FTP 域，而 FTP 域的设置则只用于相应域。如果配置的选项功能一样，则系统默认域中的相应选项继续服务器中的相应选项设置，当然也可以在域中重新配置适合本身的配置。下面分别予以介绍。

4.9.1 Serv-U 服务器的全局设置

服务器的全局设置是一些可适用于当前 Serv-U 程序中所有 FTP 域的公用设置，其中包括基本的安全设置、用户访问权限、最大上传/下载速率等。下面是具体步骤。

(1) 在如图 4-77 所示的主界面中选择“本地服务器”节点，打开的界面如图 4-78 所示。在其中显示了当前服务器的运行状态，如果正运行，则显示“服务器正在运行”。在这里还可重新配置 Serv-U 服务器是否随系统启动而启动。如果需要随系统启动而自动启动，则选择“自动开始（系统服务）”复选项。还可以通过单击【开始服务器】（当服务器当前状态为停止状态时才显示）或者【停止服务器】（当服务器当前状态为运行状态时才显示）按钮手动启动或者停止服务器的运行。



图 4-78 “本地服务器”节点配置界面

220 网管员必读——网络应用（第2版）

单击【设置/更改密码】按钮，打开如图 4-79 所示的对话框。在这里可以配置进入管理界面的管理员密码。配置密码后下次进入时就需要先输入这个密码了。首先在“旧密码”文本框中输入原来的密码，然后在“新密码”文本框中输入新的管理员密码。

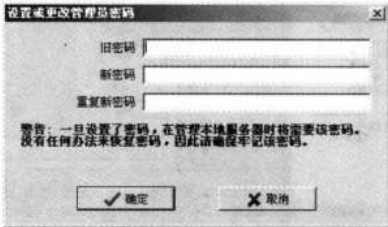


图 4-79 “设置或更改管理员密码”对话框



系统默认是不配置管理员密码的，如果重新在如图 4-77 所示的对话框中配置了管理员密码，则一定记住，因为密码丢失后是不能恢复的，否则下次就进不了管理界面了。

(2) 再在如图 4-78 所示的界面中选择“本地服务器”节点下的“设置”节点，界面如图 4-80 所示。在这里有几个选项卡，下面分别予以介绍。



图 4-80 “设置”选项界面“常规”选项卡

在“常规”选项卡中的“最大上传速度”文本框中可以设置上传文件的最大传输速率；在“最大下载速度”文本框中可以设置从 FTP 站点下载文件的最大传输速率；在“最大用户数量”文本框中可以设置 FTP 服务器上（不是针对具体的 FTP 站点）允许同时连接的最多用户数。

如果选择“检查匿名密码”复选项，则在匿名用户连接 FTP 服务器时，会检查匿名用户的密码，这样就得先为匿名用户配置密码（默认是没有密码的）；如果选择“删除部分已上传的文件”复选项，则自动删除没有上传完全的文件，以节省磁盘空间；如果不选择“禁用反超时调度”复选项，则对超过空闲等待的用户进行锁定，否则继续保持连接；如果选择“拦截‘FTP_bounce’攻击和 FXP”复选项，则仅允许 FTP 客户端与 FTP 服务器之间的连接，而阻止所有直接的 FTP 服务器对 FTP 服务器连接；如果选择“对于 XX 秒内连接超时 YY 次的用户 拦截 ZZ 分钟”复选项，则阻止在所设定的期限内（ZZ）连接超过规定次数（YY）的用户的连接，主要用于阻止那些黑客攻击。

(3) 单击“SSL 证书”选项卡，界面如图 4-81 所示。这里是用来配置 SSL 安全连接证书的，通常直接采用 RhinoSoft 公司提供的 SSL 证书即可。如果要自己配置 SSL 证书，则自己必须要有 SSL 证书服务器，通常不用另外配置。



图 4-81 “设置”选项界面“SSL 证书”选项卡

(4) 单击“目录缓存”选项卡，界面如图 4-82 所示。在这里可以设置是否启用目录缓存，以加速站点连接。如果要启用，则选择“启用缓存”复选项，然后再在“最大大小”文本框中输入最大的缓存列表数，具体要根据服务器上的内存和所缓存的内容大小而定，默认为 25 条列表。在“超时”文本框中输入缓存列表保存的最长时间，一般设置在 300 秒左右（默认为 600 秒）。时间太长，则缓存内容更新速度太慢，缓存效果不明显；如果太短，缓存内容变化太快，也起不到很明显的缓存效果。当然具体也要根据对应的 FTP 站点用户访问量来综合考虑，如果访问非常频繁，则缓存保存时间短些，否则可适当长些。如果选择“自动刷新”复选项，则在缓存列表中所列的列表项自动更新。

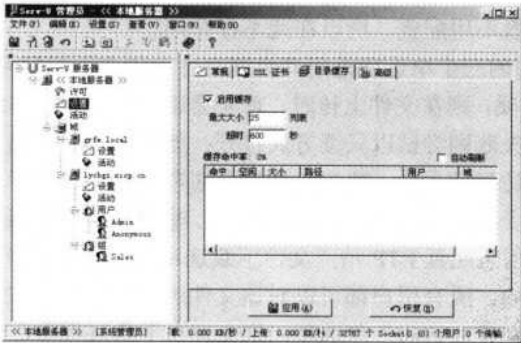


图 4-82 “设置”选项界面“目录缓存”选项卡

(5) 单击“高级”选项卡，界面如图 4-83 所示。这里的配置选项非常多。在此只介绍一些主要的。



图 4-83 “设置”选项界面“高级”选项卡

在“服务器”栏中配置的选项直接作用于 FTP 服务器，“启用安全”复选项一定要选择，特别是放在互联网上的 FTP 服务器中，否则任何人都可以进行任何操作，包括复制、更改、删除整个磁盘内容，这是非常危险的。如果选择“启用低安全性 SSL 密码”复选项，则使 FTP 服务器使用低级别（40 位，或者 56 位 DES 加密）的 SSL 加密保护，建议选择；如果选择“通过 UPnP 自动配置防火墙”复选项，则允许服务器自动搜索支持即插即用的网络设备，这些网络设备通常是路由器、防火墙之类。如果选择这一项后，在网络中有路由器或者防火墙时，就需要在这些设备上配置端口映射，否则外网用户无法访问你的 FTP 站点。通常要选择此复选项，这也就是在前面说到的防火墙、路由器设备自动识别功能。在“信息包超时”文本框中可以设置文件传输（包括上传或下载）的等待时间，当超过这个时间后便自动断开。在“目录列表掩码”文本框中配置用户访问时的默认目录列表属性，默认设置为“rw-rw-rw”，全部可读、可写，它是 UNIX 风格。通常不需要另外设置。

在“Socket”栏中可以配置 FTP 站点的套接字层，不过要注意，如果配置不当，将会使 FTP 站点陷入瘫痪。一般不用配置，所以在此不作介绍。

在“文件上传”栏中的三个单选项是用来设置文件上传方面的配置选项的，如果选择“允许无权/只读访问”单选项，则在文件上传时，首先尝试以无权方式访问其他客户和进程来打开要访问的文件，如果失败则尝试以只读方式打开；如果选择“不允许访问”单选项，则不允许在文件上传过程中访问该文件，建议选择该单选项。如果选择了“允许完全访问”单选项，则允许客户在文件上传过程中完全访问该文件，建议不要选择该单选项。

“文件下载”栏是用来配置 FTP 站点文件下载选项的，如果选择“允许完全访问”单选项，则文件在下载过程中，所有用户都可以对该文件进行完全控制方式（包括读、写权限）的访问；如果选择“允许读取访问”单选项，则文件在下载过程中，只允许用户以只读方式访问该文件，建议选择这一单选项。

（6）以上配置完成后，如果相应默认设置进行了修改，则要单击界面下部的【应用】按钮，使所做的修改设置生效。但在单击【应用】按钮前还可以通过单击【恢复】按钮恢复原来所有改变的设置。

4.9.2 Windows 账户系统的 FTP 域设置

本节要专门介绍直接采用 Windows NT 域账户的 FTP 域站点的设置方法。这类 FTP 域参

见图 4-77。下面是具体的设置方法。

(1) 在如图 4-77 所示的界面中，选择采用 Windows NT 域账户创建的 FTP 域站点（grfw.local）节点，界面如图 4-84 所示。在“域”选项卡中显示的是当前域站点的状态，绿色按钮表示域工作正常。



图 4-84 采用 Windows NT 域账户创建的 FTP 域站点界面“域”选项卡

在这里可以重新设置该站点的域名称、所用的 IP 地址、安全性和端口号。但域类型不能更改。而且更改成了非标准（FTP 服务标准的端口号为 21）的端口号后，一定要告知用户，这样用户在访问时也可做相应的更改。

如果采用默认的 21 号端口，则可不用指明端口号，直接用“ftp://FTP 域名”的格式访问，如要访问 grfw.local FTP 站点，则格式为 ftp://grfw.local。如果不是采用默认的 21 号端口，则使用如下格式：“ftp://FTP 域名:更改后的端口”，如果要采用 2100 号端口访问 grfw.local FTP 站点，则要在浏览器地址栏输入：ftp://grfw.local:2100。

如果 FTP 域名是互联网上没有固定 IP 地址的动态域名，则要选择“启用动态 DNS”复选项，此时配置界面中会多出一个“动态 DNS”选项卡，如图 4-85 所示。

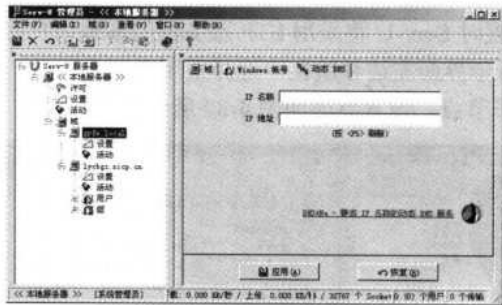


图 4-85 采用 Windows NT 域账户创建的 FTP 域站点界面“动态 DNS”选项卡

在“IP 名称”文本框中要输入 FTP 域名。需要注意的是，在“IP 地址”文本框中不用输入，系统会自动更新的，按【F5】键可手动更新。但是必须安装相应的动态域名解析服务，如在本书第 1 章所介绍的“花生壳”动态域名服务等。

(2) 选择“Winodows 账号”选项，设置界面如图 4-86 所示。在这里可以设置的选项比较多，但都是针对所采用的 Windows 账号设置的。



图 4-86 采用 Windows NT 域账户创建的 FTP 域站点界面“Windows 账号”选项卡

如果选择“将用户锁定于主目录”复选项，则所有用户只能访问所配置的主目录，不能访问其他目录，通常为了安全起见，需要选择；如果选择需要安全连接，则用户在登录前必须采用安全加密的连接方式，否则不予接受；如果选择“隐藏‘隐藏’文件”复选项，则在访问时隐藏所有有 Windows 隐藏属性的文件和文件夹，浏览时看不到；如果选择了“同一 IP 地址只允许 X 个登录”复选项，则限制在同一主机上登录 FTP 域站点的数量为 X。

在“最大上传速度”文本框中，可以设置每个用户的最大文件上传速率，不设置时为不限制；在“最大下载速度”文本框中，可以设置每个用户的最大文件下载速率，不设置时为不限制；在“空闲超时”文本框中设置允许用户空闲等待的时间，超时会自动断开相应连接，不设置时为不限制；在“会话超时”文本框中设置用户最长的连接时间，超过这个时间则自动断开连接，不设置时为不限制；在“最大用户数”文本框中可设置该 FTP 站点可以同时连接的最多用户数，不设置时为不限制；在“主目录”文本框中可以设置用户登录后进入的主目录，不设置用户登录后进入安装 Serv-U 程序 Windows 系统所在磁盘分区的根目录；在“登录消息文件”文本框中可以设置包含用户登录后显示的消息的文件，通常只能是 txt 文本格式文件，不设置时消息为空；在“Windows 域名”文本框中，选择所用的用户账户系统所对应的 Windows 域，不设置时 Serv-U 将采用 FTP 服务器的本地用户账户系统。

(3) 在如图 4-86 所示界面左边导航栏中选择采用 Windows NT 域账户系统的 FTP 域站点节点下面的“设置”子节点，设置界面如图 4-87 所示。

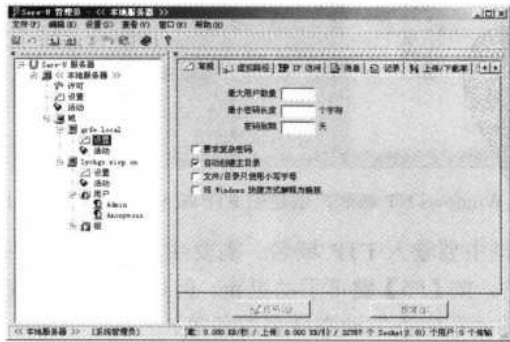


图 4-87 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“常规”选项卡

单击“常规”选项卡在“最大用户数量”文本框中可以设置该 FTP 域站点允许同时连接

的最多用户数，如果不配置则为不限制；在“最小密码长度”文本框中可以设置连接用户账户的密码最小允许的字符数，不配置则允许任意长度密码。为了用户密码安全起见，最好限制一个最小的字符数，如 6 个；在“密码到期”文本框中可以设置用户密码有效期，就像 Windows 系统中的用户账户密码有效期一样。到了有效期后，用户密码必须更换，否则用户不能再登录 FTP 服务器了。

如果选择“要求复杂密码”复选项，则要求用户密码满足一定的复杂性要求，如至少一个非数字的字符，至少一个大写字母等，与 Windows 系统中的密码复杂性策略类似。这样在为账户配置密码时一定要符合这个要求才有效。如果选择“自动创建主目录”复选项，则当用户登录 FTP 服务器时，如果发现还没有创建主目录，则自动创建主目录（默认为安装 Serv-U 程序 Windows 系统所在磁盘分区根目录），系统默认选择此复选项。如果选择“文件/目录只使用小写字母”复选项，则所有目录列表和创建的文件都以小写字母显示；如果选择“将 Windows 快捷方式解释为链接”复选项，则会在站点文件列表中 UNIX 系统的链接风格显示 Windows 快捷键目录列表。



这里所说的“主目录”要与 Windows NT 域中的用户主目录区分开来，这里的主目录仅是用户进入 FTP 站点时的根目录，不是 Windows NT 域中的用户主目录。



因为 Serv-U 的 FTP 虚拟目录创建在本章后面将专门介绍，所以如图 4-88 所示的“虚拟路径”选项卡在此不作介绍。



图 4-88 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“虚拟路径”选项卡

(4) 单击“IP 访问”选项卡，配置界面如图 4-89 所示。在这里要以添加“拒绝”或者“允许”用户访问的 IP 规则。如果要拒绝某个 IP 的用户访问该 FTP 域站点，则选择“拒绝访问”单选项，然后在“规则”文本框中键入要拒绝访问该 FTP 域站点的主机 IP 地址，或者主机名（如果是互联网上，则为相应网站的域名）。规则的格式在对话框右上角已有说明，它可以使用“*”和“?”这两个通配符，但“*”可同时用于 IP 地址和计算机名称通配，而“?”仅用于 IP 地址通配，如 192.168.9.*，grfw?，*.edu 等。如果采用 IP 地址方式，则还可以配置一个 IP 地址段，如要拒绝 192.168.2.100 到 192.168.2.200 这个地址段的主机访问，则可在规则中输入 192.168.2.100-200。最后单击【添加】按钮即可把拒绝规则添加到“IP 访问规则”列表中。如果要允许访问，则要选择“允许访问”单选项，其他配置方法与拒绝访

问规则配置一样。

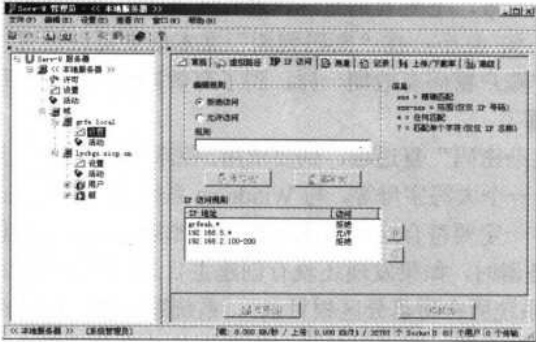


图 4-89 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“IP 访问”选项卡

在“IP 访问规则”列表中还可通过向上或向下的箭头调整规则的执行优先级。

(5) 单击“消息”选项卡，配置界面如图 4-90 所示。在这里可以配置用户访问 FTP 域站点时所显示或者弹出的各种消息。程序设置了默认配置，我们自己可以个性化设置。在“服务器响应消息”栏中配置当某一事件发生时服务器所做出的响应提示。

如在“服务器 ID 文本”中程序设置了 Serv-U 程序的版本信息，我们可以重新输入（先删除原来的）自己的服务器信息（如，grfw 公司一号 FTP 服务器之类等）；在“HELP 命令回复”文本框中可输入提供程序使用帮助电话或者邮箱之类的信息；在“服务器离线”中可输入用户在访问因某种原因暂时关闭的 FTP 服务器时所显示的消息，一般为通告；在“到达用户限制”文本框中可键入当前 FTP 站点所在线连接的用户数达到了设置限制时的通告消息；在“不允许匿名访问”文本框中输入当用户想通过不用用户账户和密码登录不允许匿名访问的 FTP 站点时所显示的警告提示；在“比率信任不足”文本框中可输入对于不符合条件的用户（证书不信任）下载时的警告提示，这主要是用于局域网中需要安全证书的情况下；在“SYST 命令回复”文本框中输入 UNIX 系统的 SYST 命令回复消息。

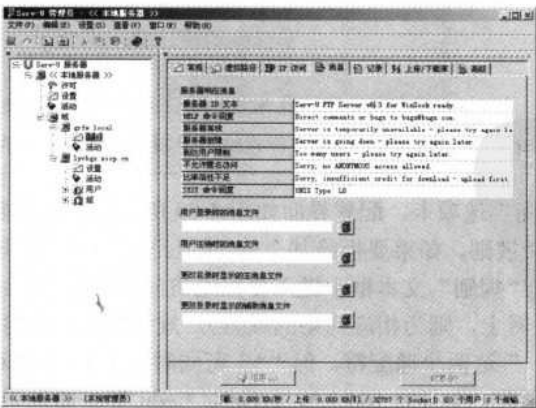


图 4-90 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“消息”选项卡

在下面这个文本框中则是用来配置用户登录或操作时的消息提示。在“用户登录时的消

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

息文件”文本框中可以配置用户登录时提示消息的文件；在“用户注销时的消息文件”文本框中可以配置用户注销登录时提示消息的文件；在“更改目录时显示的主消息文件”文本框中可以配置用户在更改目录时提示消息的文件；在“更改目录时显示的辅助消息文件”文本框中可以配置用户在更改目录和主文件未找到时提示消息的文件。这些消息文件都是.txt 格式的文本文件。

(6) 单击“记录”选项卡，配置界面如图 4-91 所示。在这里可以配置日志记录的事件、日志文件存放路径、日志文件名和日志更新频率等选项。

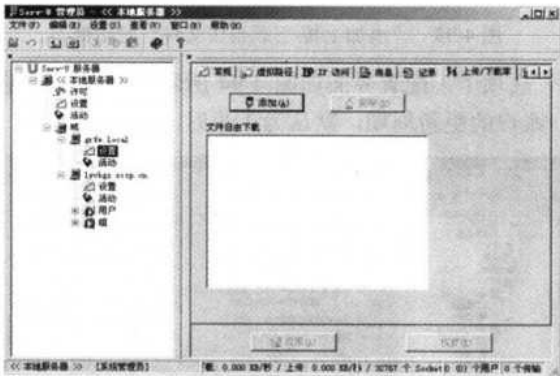


图 4-91 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“记录”选项卡

本配置界面中的选项都容易理解，在此不作介绍。

(7) 单击“上传/下载率”选项卡，配置界面如图 4-92 所示。

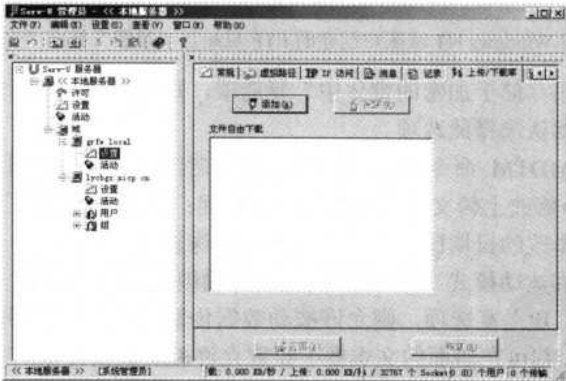


图 4-92 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“上传/下载率”选项卡

如果要允许不受 FTP 服务器通用设置的上传/下载带宽比率分配限制（参见图 4-80 所对应的设置介绍）的下载任务，则可单击界面中的【添加】按钮，打开如图 4-93 所示的对话框。在这里可以选择在 FTP 域主目录中不受上述带宽限制的下载文件路径，也可以采用像“？”和“*”这类通配符。如果仅输入文件名，没有输入路径，则这个文件可以在任何目录下，只要所下载文件的文件名一样都不受限制。这对于一些容量比较大，下载人数比较多的文件下载特别有用。选择好文件所在路径后，单击【完成】按钮即可把不受速率限制的文

件添加到“文件自由下载”列表中。

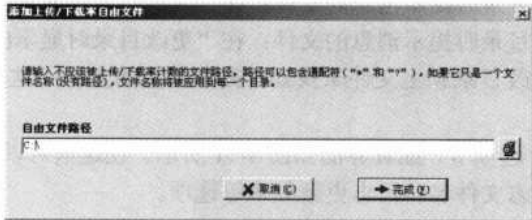


图 4-93 “添加上传/下载自由文件”对话框

(8) 单击“高级”选项卡，配置界面如图 4-94 所示。在“账号缓存活动时间”文本框中可以设置缓存中用户账户的更新周期，默认为 1 小时。

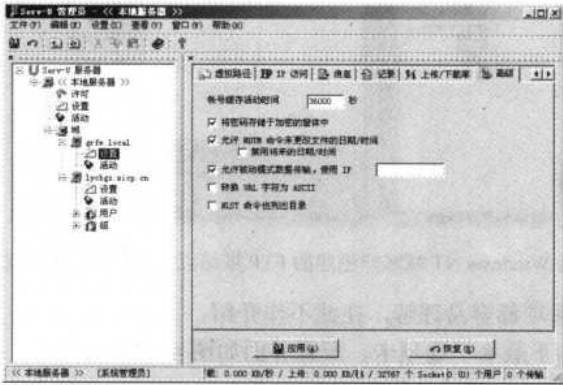


图 4-94 采用 Windows NT 域账户创建的 FTP 域站点“设置”界面“高级”选项卡

如果选择“将密码存储于加密的窗体中”复选项，则用户登录时所输入的密码将受到加密保护，更加安全，默认选择此选项。

如果选择“允许 MDTM 命令来更改文件的日期/时间”复选项，则允许具有写入权限的用户通过 MDTM 命令修改上传文件的写入日期和时间；如果同时选择了“禁用将来的日期/时间”复选项，则当修改的日期比当前日期还要晚时将忽略。

如果选择了“允许被动模式（像 Web 浏览器传输模式）数据传输（如采用 Web 浏览器方式传输数据），使用 IP”复选项，则允许被动数据传输模式，如果要限制只有个别用户可以采用被动传输模式，则可在后面的文本框中设置允许被动数据传输的主机 IP 地址，如果不设置，则允许任何用户采取被动传输模式。

注意 如果当 Serv-U 服务器位于防火墙或者代理服务器后面，则被动式传输模式不能使用，因为此时 FTP 服务器的 IP 地址所采用的是私有 IP 地址，经 NAT 转换后才与互联网连接，采用被动传输模式时，FTP 服务器不能识别。

下面两个复选项是两个很少用到命令功能，按系统默认不选择即可，在此不作介绍。完成以上配置后，单击【应用】按钮使所有改变的设置生效。不过，在单击【应用】按钮之前单击了【恢复】按钮，则本对话框中所有选项的设置都将恢复成改变以前的状态。

4.9.3 自创用户系统的 FTP 域站点设置

在 Serv-U 中，既可以创建像上节介绍的那样直接采用 Windows NT 域账户，也可以采用自创用户账户系统的方式来创建 FTP 域站点。不过，它的配置与直接采用 Windows NT 域账户的 FTP 域站点配置差不多，FTP 域及下面的“设置”配置界面选项全部一样，不同的地方只是自创用户系统 FTP 域中多了用户和组账户设置。所以，自创用户系统 FTP 域全局设置在此就不再赘述了。下节将具体介绍用户和组的相关设置。

4.10 自创用户系统的 FTP 域用户和组设置

在本节中所介绍的许多配置选项卡和配置选项与上节所介绍的全局设置一样，只是作用的对象不同而已。对于这类选项卡和选项的设置方法，在此不再另外详细介绍。



注意

如果此处的设置与前面介绍的 FTP 服务器和相应的 FTP 域设置相冲突，则最终以此处设置为准，没有冲突的相同设置选项，则向上继承。

4.10.1 用户设置

在自创用户系统的 Serv-U FTP 域中可以创建自己的用户和组账户系统，还可以针对不同的用户和组账户进行具体设置。本节介绍的是用户设置。

(1) 在如图 4-94 所示界面中，选择采用自创用户系统的 FTP 域（如本示例中的“lycbgz.xicp.cn”），然后在“用户”节点下找到要配置的用户（在此以“Admin”账户为例进行介绍，用户的创建将在本章后面具体介绍），首先见的是如图 4-95 所示的“账号”选项卡。

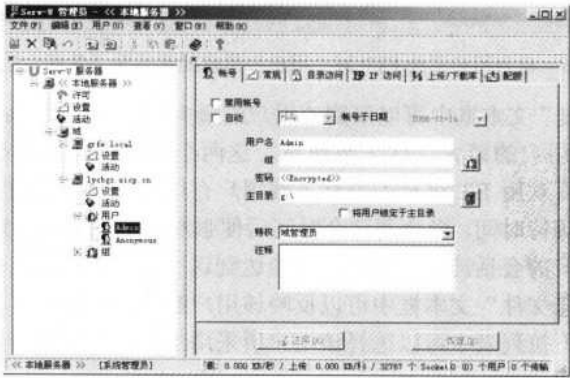


图 4-95 自创用户系统 FTP 域“用户”节点配置界面“账号”选项卡

如果要暂时禁用该账户，则可选择“禁用账号”复选项；如果选择“自动”复选项，就可以在后面的“账号于日期”滚动列表框中设置该账号在所设置的日期到达时自动删除，或者禁用。“用户名”文本框是用来设置用户账户名的，更可在此为用户改名；在“组”文本

230 网管员必读——网络应用（第2版）

框中可设置该用户所属的组，注意这里的组，是 Serv-U 自创的组，而非 Windows 系统中的组；在“密码”文本框中可以为该用户重新配置密码；在“主目录”文本框中可以设置该用户的访问主目录，这是 Serv-U 的一个明显优势所在，为用户配置主目录非常简单。

在“特权”下拉列表框中可以重新配置该用户的管理权限，同样有 5 种特权：没有特权、组管理员、域管理员、系统管理员、只读管理员。这 5 种特权说明可参见本章 4.8.2 节图 4-67 所对应的介绍。

(2) 单击“常规”选项卡，配置界面如图 4-96 所示。这个配置界面中的选项与图 4-80 所示界面类似。如果选择了“需要安全连接”复选项，则要求该用户在连接 FTP 站点时必须采取加密的连接方式，否则不拒绝连接；如果选择“隐藏‘隐藏’文件”复选项，则在该用户访问 FTP 域时，Windows 属性中配置了隐藏属性的文件将不显示；如果选择了“总是允许登录”复选项，则该用户总可以登录该 FTP 站点，即使该用户账户已过期；如果选择了“同一 IP 地址只允许 XX 个登录”复选项，则限制该用户从同一个 IP 地址发起的连接为 XX；如果选择“允许用户更改密码”复选项，则允许用户自己更改密码，通常出于安全考虑，要选择此复选项，以便用户不定期地更改自己的密码。

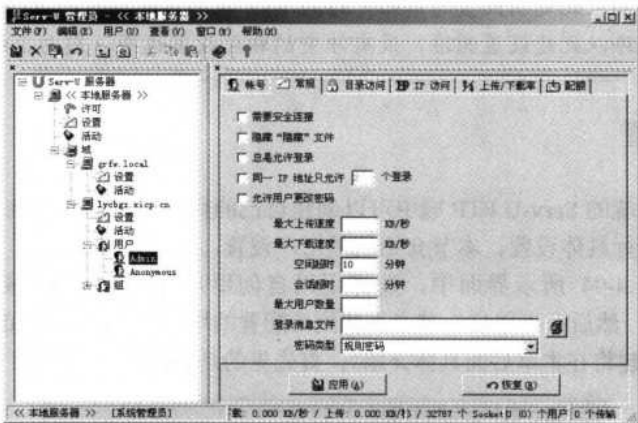


图 4-96 自创用户系统 FTP 域“用户”节点配置界面“常规”选项卡

在“最大上传速度”文本框中可以限制该用户的最大文件上传速率；在“最大下载速度”文本框中可以限制该用户的最大文件下载速率。这两个选项是用来平衡站点用户的连接性能，特别是对于目前喜欢用 BT 这样的强行下载用户有用。在“空闲超时”文本框中可以设置该用户的最长空闲等待时间，当达到这个时间后便强制中断该用户的连接；在“会话超时”文本框中可限制该用户的会话连接最长时间，当达到这个连接时间后，也会强制中断该用户的连接。在“登录消息文件”文本框中可以反映该用户的登录消息文件，实现个性的用户服务。在“密码类型”下拉列表中可以选该用户所采用的密码类型，可以是标准的密码，也可以是加密类型的密码。

(3) 单击“目录访问”选项卡，配置界面如图 4-97 所示。在这里除了可以重新设置该用户的主目录外，还可以设置该用户对该主目录中的文件的操作权限。要编辑原有主目录配置，可在列表中选择相应主目录选项，然后单击【编辑】按钮，打开如图 4-98 所示的对话框。在其中就可重新输入，或者单击后面的 按钮，在打开的窗口中选择。然后单击【完成】按

钮完成修改。

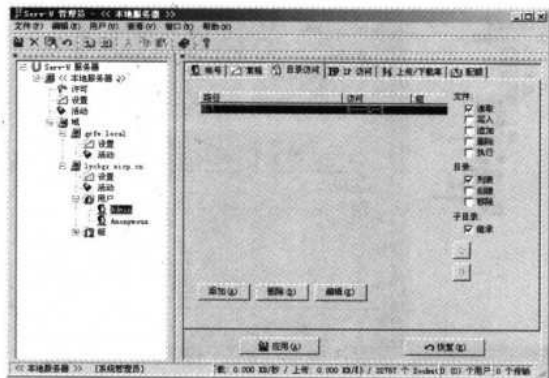


图 4-97 自创用户系统 FTP 域“用户”节点配置界面“目录访问”选项卡

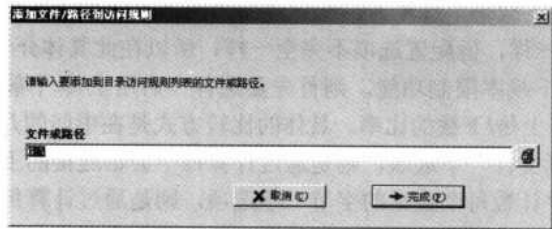



图 4-98 “添加文件/路径到访问规则”对话框

如果要删除原有主目录，则在如图 4-97 所示的对话框列表中选择相应选项，然后再单击【删除】按钮删除即可；如果要添加新的用户主文件夹，可单击对话框中的【添加】按钮，同样会打开如图 4-98 所示的对话框，可在其中直接输入，或者单击后面的  按钮，在打开的窗口中选择。最后单击【完成】按钮可完成新主目录的添加。

在如图 4-97 所示的对话框右边显示的是可为该用户配置对主目录中的文件、目录的访问权限和子目录的继承选择。

在“文件”栏中的几个权限为：读取（允许用户下载文件）、写入（允许用户上传文件）、追加（允许用户上传或在已有文件中追加新的文件）、删除（允许用户删除或更改文件）、执行（允许用户执行服务器中的程序命令）。

在“目录”栏中的几个权限为：列表（允许用户列表查看）、创建（允许用户创建新目录）、移除（允许用户删除目录）。

在“子目录”栏中有一个权限项“继承”，选择该项后允许子目录自动继承上级“目录”中所设置的上述访问权限。

(4) 单击“IP 访问”选项卡，配置界面如图 4-99 所示。这里的配置选项，与本章前面在介绍 FTP 域配置时的图 4-89 所示界面完全一样，配置方法参见即可。不同的只是作用对象不同，图 4-89 所示界面的配置选项可同时作用于中所用用户和组对象，而此处的此界面配置仅作用于具体的用户对象，在此不再赘述。

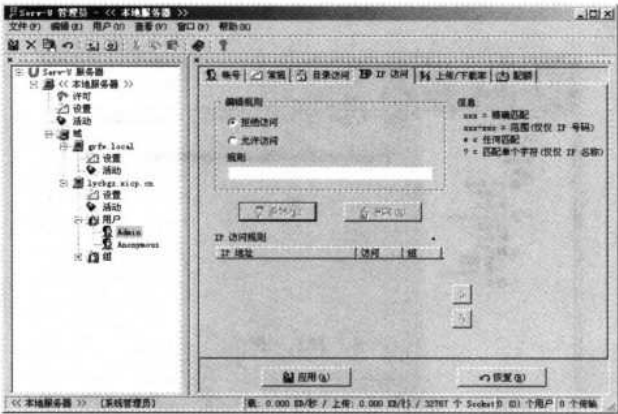


图 4-99 自创用户系统 FTP 域“用户”节点配置界面“IP 访问”选项卡

(5) 单击“上传/下载率”选项卡，配置界面如图 4-100 所示。虽然此选项卡的标题与图 4-92 的选项卡标题一样，但配置选项不完全一样，所以在此具体介绍。

要启用这项上传/下载率限制功能，则首先要选择“启用上传/下载比率”复选项，然后再在“比率”栏中选择上传/下载的比率。具体的比较方式是在中间的几个单项中选择。如果选择“计数每个会话文件”单选项，则是通过计算每个会话连接的上传或者下载文件数来比较；如果选择的是“计数每个会话的字节”单选项，则是通过计算每个上传或者下载会话连接所传输文件的字节数来比较；如果选择的是“计数所有会话文件”单选项，则是通过计算所有上传会话连接和所有下载会话连接所有传输的文件数来比较；如果选择的是“计数所有会话的字节”单选项，则是通过计算所有上传会话连接和所有下载会话连接所有传输文件的字节数来比较。在“预设/当前”栏中显示的是为该用户所预设的每个会话比率和当前的比率，通常不需要设置。

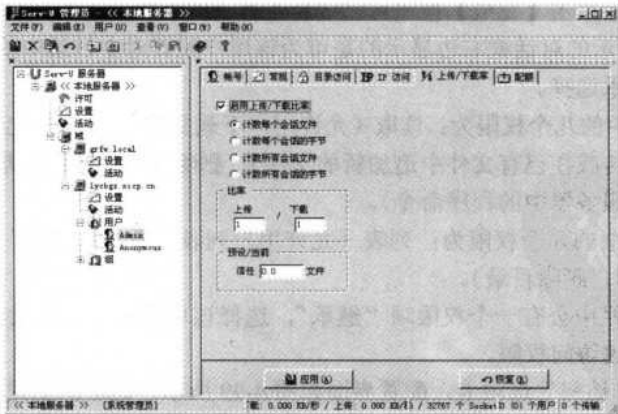


图 4-100 自创用户系统 FTP 域“用户”节点配置界面“上传/下载率”选项卡

(6) 单击“配额”选项卡，配置界面如图 4-101 所示。在这里可以为该用户配置在用户可访问目录中允许使用的最大磁盘空间，以限制该用户无限制地上传文件到 FTP 服务器中。要启用配额功能，首先要选择“启用磁盘配额”复选项，在“当前”文本框中显示的是当前

已用磁盘空间，不需要我们设置，可以直接单击【计算当前】按钮，由系统根据为该用户在如图 4-97 所示所配置的访问目录文件容量，来计算当前已使用的容量；在“最大”文本框中可配置该用户允许使用的最大磁盘空间。

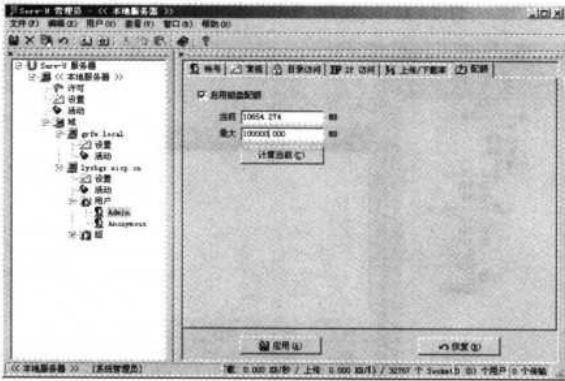


图 4-101 自创用户系统 FTP 域“用户”节点配置界面“配额”选项卡

同样，以上各项用户属性配置好后，最后需要单击界面底部的【应用】按钮保存设置，使所做的设置更改生效。当然在单击【应用】按钮前，也可以通过单击【恢复】按钮恢复当前用户以上选项卡中没有保存的更改设置选项。

4.10.2 组设置

这里的“组”是 Serv-U 中自建的组，而非 Windows 系统中的用户组。设置方法与用户的设置方法差不多。只不过，此处所做的设置将同时作用于相应组中的所有用户，而不是单独针对某个具体用户。

(1) 在如图 4-101 所示界面中选择采用自创用户系统的 FTP 域（如本示例中的“lycbgz.xicp.cn”），然后“组”节点下在找到要配置的组账户（在此以“Sales”账户为例进行介绍，组的创建将在本章后面具体介绍），首先看到的是如图 4-102 所示的“账号”选项卡。在这个选项卡没什么好设置的，只可以用来重设组账户名称和注释。

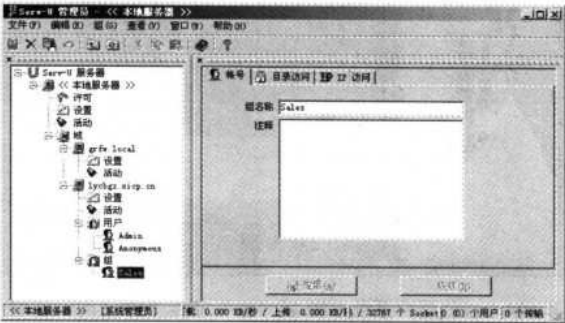


图 4-102 自创用户系统 FTP 域“组”节点“账号”选项卡

234 网管员必读——网络应用（第2版）

(2) 单击“目录访问”选项卡，配置界面如图 4-103 所示。在这里可以为组中所有用户配置可以访问的目录。同时还可以配置对这些目录和其中的文件的访问权限。这里的设置方法与上节介绍的用户目录访问（参见图 4-97）的设置方法一样，参照即可。添加目录的方法也是通过单击【添加】按钮，在打开的如图 4-98 所示的对话框中指定即可。

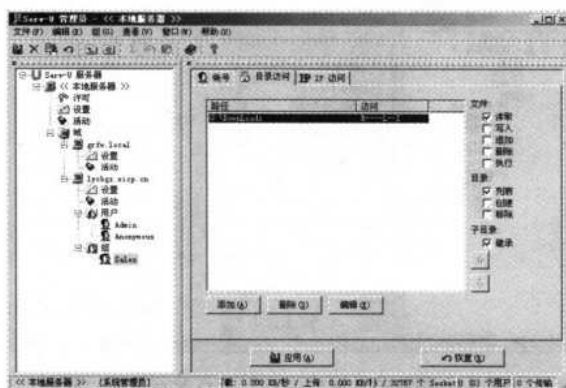


图 4-103 自创用户系统 FTP 域“组”节点“目录访问”选项卡



此处所设置的选项将同时作用于组中的所有用户，在如图 4-103 所示界面中，所添加的目录也将自动添加到所包含的用户显示在如图 4-97 所示选项卡的目录列表中，相应目录的访问权限也是依照组中的统一设置。这样，用户最终可以访问的目录就不只是在如图 4-97 所示选项卡中的用户配置的，还要结合所隶属的组中的目录设置。如某用户在如图 4-97 所示选项卡添加的目录为“c:\d\”，而在他所隶属的一个组中添加了“e:\”访问目录，则该用户最终可访问的目录就是“c:\d\;e:\”这三个了。

(3) 单击“IP 访问”选项卡，配置界面如图 4-104 所示。这个选项卡的配置也与 4-99 所示选项卡的配置方法一样，设置方法参照即可，不再赘述。

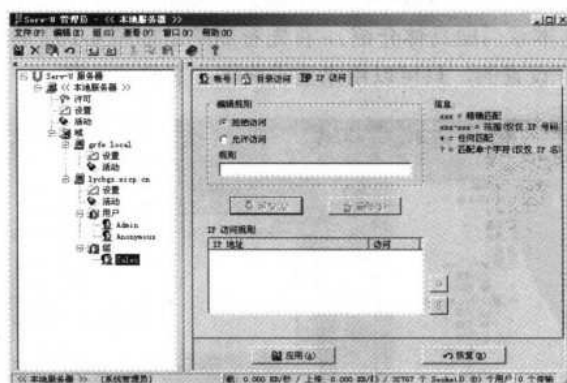


图 4-104 自创用户系统 FTP 域“组”节点“IP 访问”选项卡

以上就是组账户的全部设置过程，相对用户来说要简单许多。下面具体介绍 Serv-U 中的虚拟目录、用户和组创建方法。

4.11 虚拟目录、用户和组创建

在 Serv-U 中，与 IIS 一样，也可以添加不在本地 FTP 服务器主目录中的其他目录作为虚拟目录，该虚拟目录的实际物理位置可以是在本地服务器上，也可以在网络中的其他计算机上。另外，在自创用户系统的 FTP 域中，还需要用 FTP 域创建用户和组账户。也可以创建用于匿名访问的账户，但在直接采用 Windows 用户系统的 FTP 域中不可创建匿名访问的用户账户，也就不支持匿名访问了。

4.11.1 虚拟目录创建

在 Serv-U 中，虚拟目录可以在 FTP 域站点中创建，它包括两种：虚拟路径和虚拟链接。下面分别予以介绍。

1. 虚拟路径创建

(1) 在 Serv-U 主界面中，打开要创建虚拟路径的 FTP 域站点，在详细列表信息窗口右边的配置界面中选择“虚拟路径”选项卡，如图 4-105 所示。

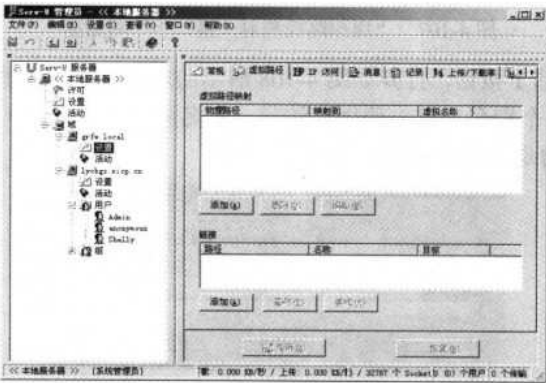


图 4-105 FTP 域“设置”界面“虚拟路径”选项卡

(2) 在“虚拟路径映射”列表下面单击【添加】按钮，打开如图 4-106 所示的对话框。在其中要指定新创建的虚拟目录的实际物理路径。可以是本机上的，也可以是网络磁盘中。

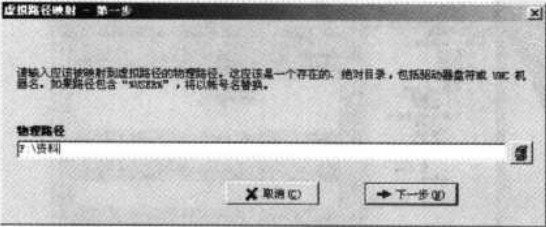


图 4-106 “虚拟路径映射—第一步”对话框

(3) 单击【下一步】按钮，打开如图 4-107 所示的对话框。在这里可以指定上一步配置

的物理路径所指向的虚拟路径。这个目录可以是空的（也就是说可以不包括任何文件），这样可以有效保护上一步物理路径的安全，因为通过此步的指定就可使访问者认为上一步所指的物理路径为此处指定的虚拟路径。当然此处的路径也必须是存在的，同样既可以是本机上的，也可以是网络磁盘上的。用“%home%”可以代替相应用户的主目录，不同用户的主目录不同，用户在访问时就用相应的用户主目录替换；而“%USER%”则可替代用户的账户，如在“Documet and Settings”文件夹下就有不同用户的文件夹，如果虚拟目录指向这里的话，则可以用“%USER%”来替换不同用户所对应的文件夹。不使用路径变量“%HOME”和“%USER%”时所指定的虚拟路径是固定的，而如果使用了这两个路径变量，则非常灵活，不同用户所对应相同的物理路径的虚拟路径可以不一样，因为不同的用户主目录可能不一样，如果固定的话，当所指定的固定路径不是所有用户都可以访问时，有些用户就不能访问这个虚拟路径下的文件了。

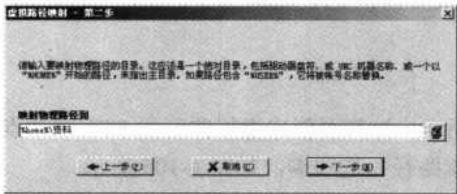


图 4-107 “虚拟路径映射—第二步”对话框

(4) 单击【下一步】按钮，打开如图 4-108 所示的对话框。在这里可以为该虚拟路径在相应 FTP 域中配置一个别名，以方便用户访问。别名应该简短。上一步设置的虚拟路径在 FTP 站点中最终显示的是此处配置的别名。

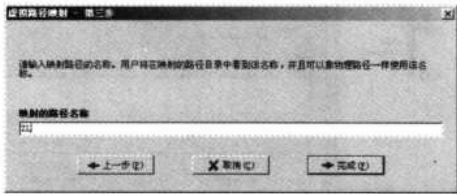


图 4-108 “虚拟路径映射—第三步”对话框

(5) 单击【完成】按钮，完成虚拟目录的创建。此时新建的虚拟目录就会在如图 4-105 所示的“虚拟路径映射”列表框中显示，如图 4-109 所示。



图 4-109 在“虚拟路径映射”列表框中显示的新建的虚拟路径

2. 虚拟链接创建

虚拟链接是为了给实际存在的链接资源提供虚拟映射，以便用户访问。其实就相当于链接本身的作用。如在 FTP 站点加上友情链接，就可以通过这一方法来实现，而且还不用手工一个个来创建。具体创建的步骤如下。

(1) 在如图 4-109 所示选项卡的“链接”列表中单击【添加】按钮，打开如图 4-110 所示的对话框。在这里可以为新创建的虚拟链接指定在 FTP 站点中显示的路径，如果不指定，则在 FTP 站点中所有目录中显示，这一功能非常有用，如要在每个用户访问目录中显示公司网站链接，就不需要在每个目录下一一添加了，只需在这里设置即可。

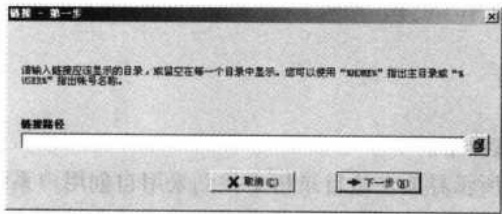


图 4-110 “链接—第一步”对话框

(2) 单击【下一步】按钮，打开如图 4-111 所示的对话框。在这里要为该虚拟链接配置一个链接名，这个链接名也是用来在 FTP 站点中显示的。

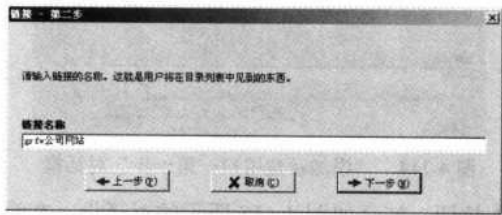


图 4-111 “链接—第二步”对话框

(3) 单击【下一步】按钮，打开如图 4-112 所示的对话框。在这里要指定该虚拟链接所指向的真实链接地址。

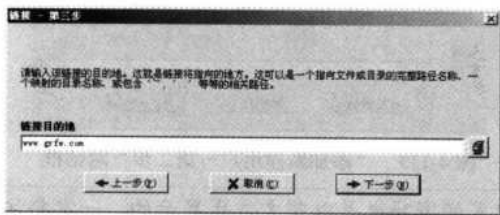


图 4-112 “链接—第三步”对话框

(4) 单击【下一步】按钮，即完成虚拟链接的创建。创建后同样会在如图 4-113 所示的对话框中显示。

有关于 Serv-U FTP 站点的配置就介绍至此。



图 4-113 在“链接”列表框中显示的新建的虚链接

4.11.2 用户账户创建

用户账户创建的步骤如下。

(1) 在如图 4-113 所示界面左边目录树中找到采用自创用户系统的 FTP 域，然后选择“用户”节点，单击鼠标右键，在弹出的快捷菜单中选择【新建用户】命令，打开如图 4-114 所示的对话框。在这里要输入创建的用户账户名，这个账户名必须是同一个 FTP 服务器上唯一的，也就是说不能使用当前 FTP 服务器中其他 FTP 域中已有的用户名称。

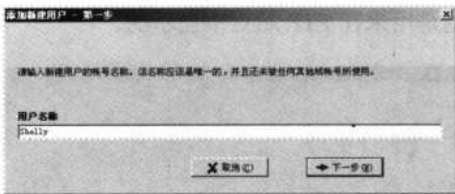


图 4-114 “添加新建用户—第一步”对话框

(2) 单击【下一步】按钮，打开如图 4-115 所示的对话框。在这里要为上面创建的用户账户配置密码。这里的密码一定要符合在上面 FTP 域属性配置中的密码复杂性要求设置，参见图 4-86。

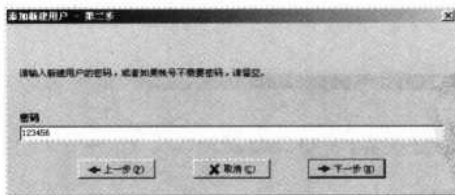


图 4-115 “添加新建用户—第二步”对话框



注意

这里配置的密码也是以明文方式显示的，一定要注意保密。另外，如果在上一步创建的是匿名访问用户账户（匿名账户名指定为 anonymous，不能改），则在如图 4-114 所示的对话框中单击【下一步】按钮后，不会出现如图 4-115 所示的对话框，而是直接进入下一步如图 4-115 所示的对话框。

(3) 单击【下一步】按钮，打开如图 4-116 所示的对话框。在这里要为该用户在 FTP 域中配置访问的主目录。主目录是用户连接 FTP 站点后首先进入的目录。不同用户可以有各自不同的访问主目录，也可以有许多用户都是同样的主目录。这主要根据实际应用需求和权限来设置。

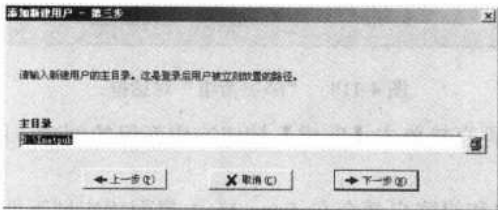


图 4-116 “添加新建用户—第二步”对话框

(4) 单击【下一步】按钮，打开如图 4-117 所示的对话框。在这个对话框中要选择是否要把用户访问的范围锁定在主目录中。也是根据不同用户而定，一般普通用户，则最好锁定（选择“是”单选项），对于具有较高权限的用户和配置了多个访问目录（参见图 4-97），则不要锁定（选择“否”单选项），否则虽然在如图 4-97 所示选项卡中配置了其他访问目录，仍不能访问。

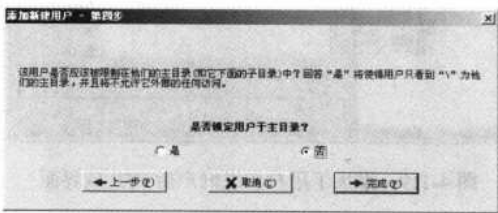


图 4-117 “添加新建用户—第三步”对话框

(5) 单击【完成】按钮，完成一个用户账户的创建。创建用户后，可以对具体用户属性和对 FTP 站点的访问进行选项配置，具体参见 4.10.1 节的介绍。

4.11.3 组账户的创建

有时我们需要在 FTP 站点中为不同类型的用户配置相同的访问权限和主目录，特别是在单位内部的 FTP 站点中，如为不同部门的员工配置相同的主目录，相同的访问属性。这时，如果仍像上节那样为每个用户一一配置的话，就非常麻烦了。此时我们可以像 Windows 系统那样，采取工作组的方式对同类型的用户集中配置。下面是 Serv-U 组账户的具体创建步骤。

(1) 在如图 4-113 所示界面左边目录树中找到采用自创用户系统的 FTP 域，然后选择“组”节点，单击鼠标右键，在弹出的快捷菜单中选择【新建组】命令，打开如图 4-118 所示的对话框。在这里要输入创建的组账户名，这个账户名也必须是同一个 FTP 服务器上唯一的。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

240 网管员必读——网络应用（第2版）

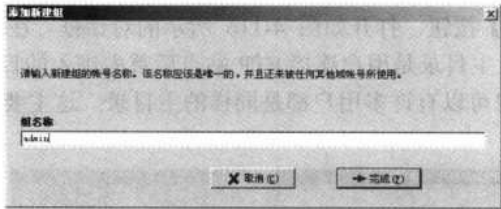


图 4-118 “添加新组”对话框

（2）输入组名后，再直接单击【完成】按钮完成新组的创建。同样可以按 4.10.2 节中介绍的方法配置组选项。

以上两节新建的用户和组账户都会在 Serv-U 主界面相应域下面的“用户”或“组”点中出现，如图 4-119 所示。

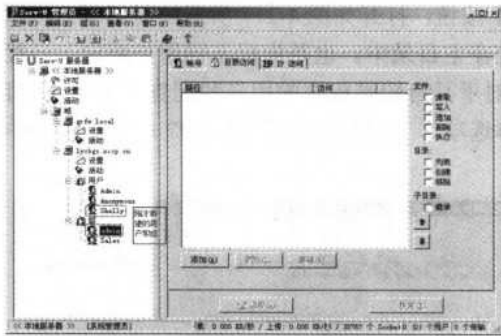


图 4-119 添加了用户和组账户后 FTP 域界面

4.12 FTP 站点的访问与管理

本章最后介绍一下 FTP 站点的访问与管理方法，它同时适用于 IIS FTP 站点和 Serv-U FTP 站点。

4.12.1 FTP 站点的终端客户访问

一般来说，FTP 站点的终端客户访问是直接浏览器地址栏中输入 FTP 站点地址（可以是域名，也可以是 IP 地址），但 FTP 站点的访问多数是直接采用 IP 地址进行的。在 IIS FTP 站点中还没有把 FTP 站点的 IP 地址与域名进行关联，所以访问 IIS 中的 FTP 站点时只能通过 IP 地址进行。在 Serv-U 中，FTP 站点的 IP 地址是与域名关联的，所以既可以使用 FTP 站点 IP 地址，也可以使用 FTP 站点域名访问。

如果 FTP 站点采用标准的 21 号端口来访问，则用户在访问时就无须加上端口号，直接在浏览器地址栏中输入“ftp://xxx.xxx.xxx.xxx”（此为 FTP 站点的 IP 地址，根据实际 FTP 站点配置也可以采用 FTP 域名）；如果不是采用默认的 21 号端口，如采用了 2100 号端口，则要在浏览器地址中输入“ftp://xxx.xxx.xxx.xxx:2100”，也就是指定端口号。

在浏览器地址栏中输入正确的地址后，如果 FTP 站点没有配置匿名访问账户，也就是不允许匿名访问，则会打开如图 4-120 所示的对话框，要求输入用户账户信息，然后单击【确定】按钮，进入到相应用户在 FTP 站点中配置的主目录中，如图 4-121 所示。如果配置了匿名访问，则直接在浏览器中输入 FTP 站点地址，是不会出现如图 4-120 所示的对话框的，而是直接以匿名身份方式进入匿名用户主目录。这一点要格外注意。如果要在 FTP 站点中既允许匿名访问，又要允许其他高级用户以特权访问，则不能直接在浏览器地址输入地址来访问了，而是采用专门的 FTP 站点管理工具进行了，如下节将要介绍的 CuteFTP 等。

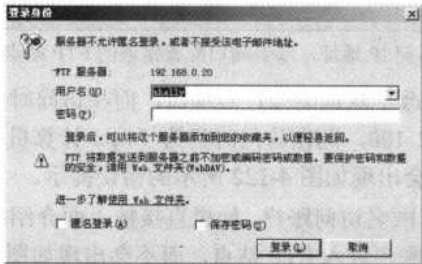


图 4-120 “登录身份”对话框



图 4-121 在浏览器地址中输入地址后进入的相应用户主目录

进入主目录界面后，用户就可以像在本地资源管理器中进行文件操作一样，进行用户相应权限的文件操作。具体当前用户对相应目录具有哪些操作权限可以通过在相应文件夹或文件上单击鼠标右键，在打开的快捷菜单中了解到。在这个快捷菜单中有些命令是在本地资源管理器中操作所没有的，那就是“复制到文件夹”，这个文件夹就可以把所选文件夹或文件下载到用户指定的目录中。

如果是在 FTP 站点界面空白处单击鼠标右键，则在快捷菜单中有一个【登录】命令也是在本地磁盘资源管理器中单击鼠标右键所没有的，它是用来改变当前登录用户的。



在 FTP 主界面中只看到相应用户的主目录，其他所添加的虚拟目录并没有在界面中显示，如何进入访问、操作呢？这时可以通过直接在 IE 浏览器地址栏输入 FTP 站点 IP 地址时加上这个虚拟目录别名即可，如 `ftp://192.168.0.20/zl`。

如果在 FTP 服务器中有多个 IP 地址，而在浏览器中输入的 IP 地址与相应 FTP 站点配置的 IP 地址不一致时，则不能登录成功。但在不指定具体的 IP 地址的情况下（把相应 FTP 站点当做默认的 FTP 站点），只要所输入的 IP 地址是 FTP 服务器计算机中的一个 IP 地址，都

242 网管员必读——网络应用（第2版）

可登录成功。但如果在 FTP 站点属性配置中指定的 IP 地址不正确（如本来是采取了动态 IP 地址分配方式，却指定一个静态的 IP 地址，或者 FTP 站点本来是放在互联网上，却指定了一个局域网 IP 地址），用户访问时都会弹出如图 4-122 所示的错误提示。这是一种非常典型的错误，提示中的“与服务器的连接被重置”是经常遇到的，许多网友都不知道错误在哪里。

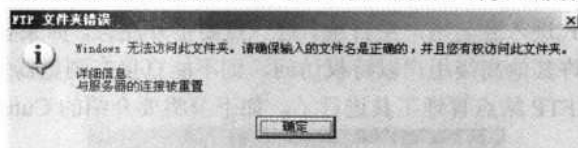


图 4-122 访问 IP 地址，或者端口配置错误的 FTP 站点的错误提示

还有一种情况，就是更改了默认的 21 号端口，而在访问时并没有加上这个端口号，如把默认的 21 号端口改成为 2100，而在访问时仍为“ftp://计算机名（或 IP 地址）”，没有加上“:2100”，在访问时同样会出现如图 4-122 所示的错误提示。

如果某 FTP 站点配置了匿名访问账户，如果直接按上面介绍的方法在浏览器地址栏输入地址的话，就会直接以匿名账户进入 FTP 站点，而不会出现如图 4-120 所示的登录身份对话框。此时，如果要特权用户登录，则需要采用一种配带用户账户的地址，即“ftp://用户账户@FTP 服务器计算机名（或 IP 地址）”，如 shelly 用户要登录笔者的 FTP 服务器，则可在 IP 地址栏中输入“ftp://shellyg@grfw-s1”或者“ftp://shelly@192.168.0.20:2100”。如果 FTP 站点中采用的是域网络的用户账户，则此时的账户一定要在域控制器上已经创建，并且当前有效。这样输入地址后，就同样可以打开如图 4-120 所示的对话框，在其中输入特权用户账户和密码即可以特权身份连接 FTP 站点。



以上各种格式中并没有加上访问 FTP 站点的端口号，是因为采用了 FTP 访问默认的 21 号端口。同样，如果端口进行了更改，则一定要加上，如改为 2100，则以上访问格式就应为：ftp://grfw-s1:2100、ftp://192.168.0.20:2100 或者 ftp://shelly@grfw-s1:2100 等。

4.12.2 FTP 站点的远程连接

如果 FTP 服务器是放在其他 ISP 中进行托管，或者 FTP 站点是放在其他 ISP 的服务器上，企业管理员就不可能到 FTP 服务器本地进行管理，这时就得依靠一些 FTP 站点管理工具了。其中典型代表就是 CuteFTP，可以在其官方网站 <http://www.globalscape.com/>，或者其他下载网站上下载试用版。目前其专业版的最新版本为 8.0，它不仅可用 FTP 站点连接，还可用 FTPS、HTTP、HTTPS 和 SSL 等安全 FTP 和 HTTP 连接。

在程序安装后，CuteFTP 可以配置 FTP 站点的连接，当然也可以在此先不进行连接，而在 CuteFTP 界面中通过新建连接来配置。

在 CuteFTP 中，连接已有 FTP 站点的方法有两种，一种是向导方法；另一种是新建方式。下面分别予以介绍。

1. 利用向导方式与 FTP 站点远程连接

(1) 运行所安装的 CuteFTP Professional，打开如图 4-123 所示的主界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 在左上角窗口中的“General FTP Sites”选项上单击鼠标右键，在弹出的快捷菜单中选择【Connection Wizard】命令，打开如图 4-124 所示的对话框。在这里要新建的远程 FTP 站点连接指定一个 IP 地址和站点名称，IP 地址必须正确，但站点名称不一定要与远程 FTP 站点一样，可随意取。但因为这里没有指定所用端口号，所以，在此只能连接采用 21 号端口的 FTP 站点。



图 4-123 CuteFTP Professional 主界面



图 4-124 配置远程连接名称对话框

(3) 单击【下一步】按钮，打开如图 4-125 所示的对话框。在这里要输入有权连接此 FTP 站点的用户账户信息。因为管理 FTP 站点通常为 FTP 站点管理员，所以在此要输入远程 FTP 站点管理员账户信息，或者其他具有特权的用户。当然这个管理员账户一定要在远程 FTP 站点中已配置好。

(4) 单击【下一步】按钮，打开如图 4-126 所示的对话框。在这里要指定该用户与远程 FTP 站点连接后默认进入的本地路径和远程 FTP 站点路径。通常本地路径（在“Default Local Folder”下拉列表框中选择）是指向相应用户的配置文件用户主文件夹中，当然也可以随意更改。而在远程 FTP 站点中的路径（在“Default Remote Folder”文本框中指定）一般是对应用户可以访问的主目录，事先已在 FTP 站点中配置好。如果不清楚在远程 FTP 站点的主目录路径，则可以不填写，让系统自动定位。



图 4-125 配置管理员账户信息



图 4-126 指定用户登录 FTP 站点后的默认本地磁盘路径和远程 FTP 站点路径

(5) 单击【下一步】按钮，打开如图 4-127 所示的向导完成对话框。单击【完成】按钮，即开始与远程 FTP 站点连接，成功后，即在 CuteFTP Professional 主界面窗口中显示上一步

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

244 网管员必读——网络应用（第2版）

或者 FTP 站点设置的主目录，如图 4-128 所示。



图 4-127 向导完成对话框

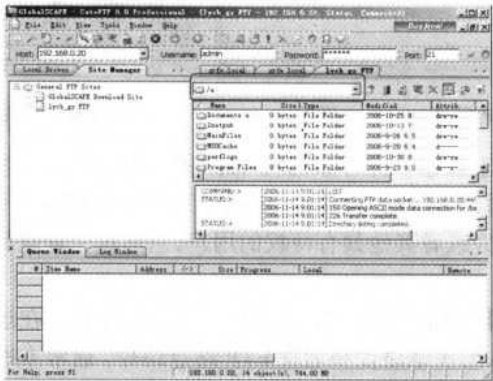


图 4-128 远程 FTP 站点连接成功后的“Site Manager”选项卡

还可以通过对应窗口上部的下拉列表框调整要查看的远程 FTP 站点目录位置。如果要在上一步所指定的用户默认本地路径文件，则可在如图 4-128 所示界面左边窗口中单击“Local Drivers”选项卡，在左边窗口中即显示相应用户的本地磁盘中的默认路径，如图 4-129 所示。在其下面也有一个下拉列表，可以调整要查看的本地磁盘位置。

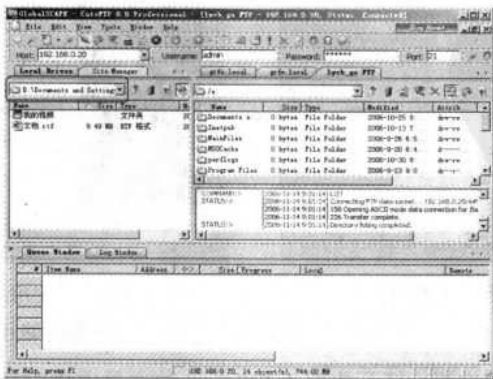


图 4-129 远程 FTP 站点连接成功后的“Local Drives”选项卡

2. 新建 FTP 站点法

除了可以采取以上向导方式与远程 FTP 站点连接外，还可采取新建 FTP 站点的方式进行，具体步骤如下。

(1) 在如图 4-128 所示 CuteFTP 主界面的“General FTP Sites”节点上单击鼠标右键，在弹出菜单中选择【New】下的【FTP Site】命令（当然如果采取加密方式的 FTP 站点，则需要选择【FTPS (SSL) Site】，或者【SFTP (SSH2) Site】命令；如果是基于 HTTP，或者 HTTPS 协议的 FTP 站点，则可选择【HTTP Site】，或者【HTTPS (SSL) Site】命令，在此仅选择【FTP Site】命令为例进行介绍），打开如图 4-130 所示的对话框。

在这里，你可以配置新建的 FTP 站点基本属性，“Lable”文本框中可以输入新建 FTP 站点的名称。不过，这里同样可以不是实际 FTP 站点的名称，只是用来在 CuteFTP 界面上标识。在“Host address”文本框中可以输入 FTP 站点对应服务器的 IP 地址，或主机名，如果是放在互联网上的，则一定要输入合法的公网 IP 地址，或者域名（在采取动态域名解析方式时，则必须输入域名）；在“Username”文本框中输入要与远程 FTP 站点连接的用户名；在“Password”文本框中输入相应连接用户账户的密码。在“Login method”栏中可以选择登录的方式，可以普通（Normal）的，也可以是匿名（Anonymous）的，也可以是两者均可以（选择“Double”单项）。

对于一般的远程 FTP 站点连接，其他几个选项卡可不用配置，但如果想要对该 FTP 站点的其他特权用户访问选项进行配置的话，则可以适当配置。在此仅对主要选项进行介绍。

(2) 单击“Type”（类型）选项卡，对话框如图 4-131 所示。在“Protocol type”（协议类型）下拉列表框中可以选择新站点所用的传输协议，要根据对应 FTP 站点所用协议来选择。后面的“port”（端口）文本框中也一样，但必须使用与远程站点一致的协议端口。在前面介绍的 FTP 连接创建方法中不能指定连接 FTP 站点的端口，在此处就可以了。对于不是使用默认的 21 号端口的 FTP 站点连接的话，这种连接方式是必须的选择。可以改为其他端口，当然这个端口必须与相应 FTP 站点的端口配置一致。



图 4-130 新建站点配置对话框“General”选项卡



图 4-131 新建站点配置对话框“Type”选项卡

至于下面的“Server type”（服务器类型）、“Data connection type”（数据连接类型）、“Transfer

246 网管员必读——网络应用（第2版）

type”（数据传输类型）、“Server time zone”（服务器时区）这几项的设置通常是按远程 FTP 站点的服务器配置，具体在此不作介绍。

在“Password Protection”栏中是用来选择用户密码保护方式：“No Encrypted”（无加密）、“MD4”（版本 4 的消息摘要模式）、“MD5”（版本 5 的消息摘要模式）、“Auto detectOT”（自动检测）。

(3)单击“Actions”(行为)选项卡,对话框如图 4-132 所示。在“When client connects,switch to this remote”文本框中指定当客户端连接时，统一切换到下面指定的远程目录中，而不是根据用户主目录设置自动进入各自的主目录中。

在“When client connects, switch to this local folder”文本框中指定当客户端连接时，统一切换到下面指定的本地目录中。在“For navigation use the following caching options”下拉列表框中可以选择是否采用缓存，使用缓存的好处就是可以本机上存储网站列表，当不能连接到 FTP 服务器时仍可以查看相应列表信息。如果选择“Use cache during seesion”选项，则在会话过程中使用缓存；如果选择“Always use cache”选项，则总是使用缓存；如果选择“Do not use cache”选项，则不使用缓存。在“When uploading, apply this rule to files and”下拉列表中选择上传文件规则，如果选择“Preserve case”选项，则上传文件名仍保持原样；如果选择“Force lower case”选项，则强迫上传文件的文件名改为小写字母；如果选择“Force upper case”选项，则强迫上传文件的文件名改为大写字母。

单击【Filter】按钮，打开如图 4-133 所示的对话框。在这里可以设置在 FTP 站点上文件显示过滤，让有些符合条件的文件不在站点中显示。不过首先要选择“Enable filtering”（启用过滤）复选项，才可以配置下面的各过滤项。具体不作介绍。



图 4-132 新建站点配置对话框“Actions”选项卡



图 4-133 “Filter”对话框

(4) 在如图 4-132 所示的对话框中单击“Options”选项卡，对话框如图 4-134 所示。在这里可以选择一种站点属性配置方式，在“Site specific configuration options”（站点专门配置选项）下拉列表中有两个可选项。

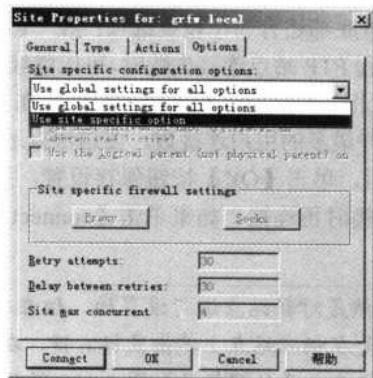


图 4-134 新建站点配置对话框“Options”选项卡

如果选择“Use global settings for all options”选项，则新建站点将采用在 CuteFTP 中为所有站点设置的所有全局配置选项（具体将在本章后面介绍）；如果选择“Use site specific option”选项，则可在该对话框中为该新建站点专门配置选项，激活下面未激活的选项。如果选择“Apply auto-rename scheme to transfer”复选项，则所传输的文件将按全局配置中的文件重命名规则进行名称转换，否则传输的文件名不作更改；如果选择了“Use NLST instead of LIST（retrieves an abbreviated listing）”复选项，则在站点中向用户显示的仅是文件名列，而不包括诸如大小、文件夹名称、修改日期等信息。如果选择“Use the logical parent（not physical parent）on CDUP”复选项，则当单击按钮时会返回到上一级目录，即使所单击的按钮是一个链接，或者快捷键。通常不选择这个复选项。

在“Site Specific Firewall settings”栏中，可以设置站点的防火墙选项，但这里要注意的是，这里所说的“防火墙”并不是真正意义上的防火墙，而是对诸如代理服务器，或者套接字层服务器进行配置。如果当前需要通过代理服务器与远程 FTP 站点连接，则单击【Proxy】按钮，打开如图 4-135 所示的对话框，在这里可以配置代理服务器，其中包括代理服务器类型、服务器地址、与远程 FTP 站点连接的用户账户信息；如果要通过套接字层（Socks）服务器与远程 FTP 站点连接，则单击如图 4-134 所示的对话框中的【Socks】按钮，打开如图 4-136 所示的对话框。在其中同样可以配置 Socks 服务器类型、服务器地址、与远程 FTP 站点连接的用户账户信息等。需要注意的是，在图 4-135 和图 4-136 两个对话框中的服务器端口建议不要更改，因为这是默认的相应服务所用端口号。



图 4-135 “Proxy”对话框

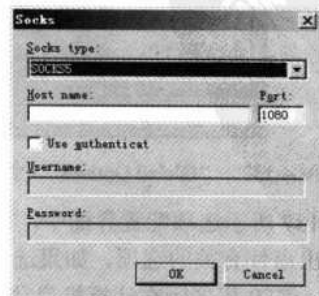


图 4-136 “Socks”对话框

248 网管员必读——网络应用（第2版）

在如图 4-134 所示的对话框底部还有 3 个设置选项：在“Retry attempts”文本框中，可设置用户通过 CuteFTP 软件与远程 FTP 站点连接失败时，可以继续尝试的次数；在“Delay between retries”文本框中可以设置两次相邻登录尝试相间隔的时间；在“Max connections per this site”文本框中可以设置一个站点允许最多的用户连接数，要这根据远程 FTP 站点的性能配置而定。

（5）以上设置全部完成后，单击【OK】按钮保存设置，只在 CuteFTP 中新建站点，但并不连接，可以在以后需要连接时再连接。如果单击【connect】按钮，则立即开始与所新建的站点连接。



以上配置虽然是对新站点进行设置的，但在已有站点中同样可以进行以上属性设置。方法是在相应站点上单击鼠标右键，在弹出菜单中选择【Properties】（属性）命令，首先打开的同样是如图 4-130 所示“General”（常规）选项卡对话框。

另外，对于 IIS 中的 FTP 站点，同样可以通过“远程管理（HTML）”管理工具进行远程管理，具体方法参见第 2 章相关内容。

4.12.3 CuteFTP 的站点全局配置

在前面我们说到，在新站点属性配置中，在如图 4-97 所示的“Options”选项卡中，可以全部采用 CuteFTP 中为所有站点设置的全局配置。现在就来介绍一下，在 CuteFTP 中如何为所有站点设置全局配置。主要步骤如下。

（1）在 CuteFTP 主界面中执行【Tools】→【Options】菜单操作，打开如图 4-137 所示配置窗口。这是一个导航式的选项配置窗口。从这里可以看出，可以配置的选项非常多。限于篇幅的原因，在此不可能一一介绍，只能对一些主要属性选项（主标签）配置进行介绍。

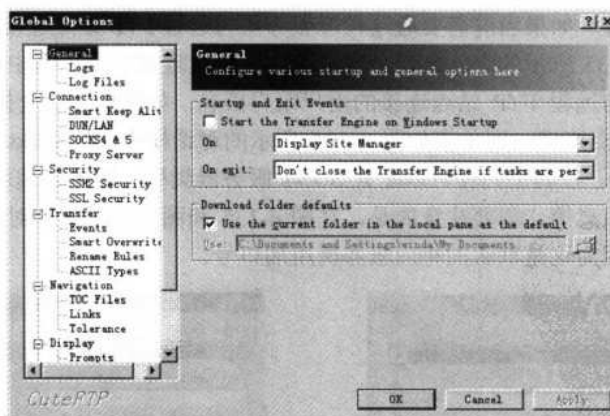



图 4-137 “Global Options”（全局选项）对话框“General”选项配置界面

在如图 4-137 所示选项配置界面中，在“Startup and Exit Events”栏中，可以配置与传输任务启动和退出事件有关的选项。如果选择了“Start the Transfer Engine on Windows Startup”选项，则在 CuteFTP 程序所在计算机启动后便自动启动文件传输任务。

在“On”下拉列表中有 3 个可选项：如果选择“Display Site Manager”选项，则在程序

启动时显示站点管理器；如果选择“Do Nothing”选项，则在程序启动时站点管理器保持不变；如果选择“Connect to the last connected to Site Manager”选项，则自动连接到上一次退出前所连接的站点。

在“On exit”下拉列表中，如果选择“Don't close the Transfer Engine if tasks are pending”选项，则当程序退出时如果仍有传输任务未完成时继续传输，则不关闭传输引擎的运行，直到所有任务完成后自己退出程序；如果选择“Don't close the Transfer Engine”选项，则不关闭传输引擎的运行，即使 CuteFTP 程序关闭，或者没有传输任务，直到计算机的关闭，或者手动从系统状态栏关闭 CuteFTP 传输引擎；如果选择“Close the Transfer Engine”选项，则在关闭 CuteFTP 程序时，停止传输引擎的运行。

在“Download folder defaults”栏中可以设置下载文件默认的存放位置。如果选择了“Use the current folder in the local pane as the default”，则把当前 CuteFTP 程序主界面中的“Local Drivers”窗口中显示的文件夹为下载文件默认的存放位置。如果取消该复选项的选择，则下面的文本框将激活，可直接在其中输入默认路径，也可通过单击后面的  按钮定位查找。

(2) 单击“General”项下的“Logs”选项，配置界面如图 4-138 所示。在“Log text colors”栏中可以设置不同日志记录文本的颜色。在“Log text fonts”栏中可以设置日志文本的字体和字号大小。单击【select Font】按钮，在打开的对话框中选择即可。

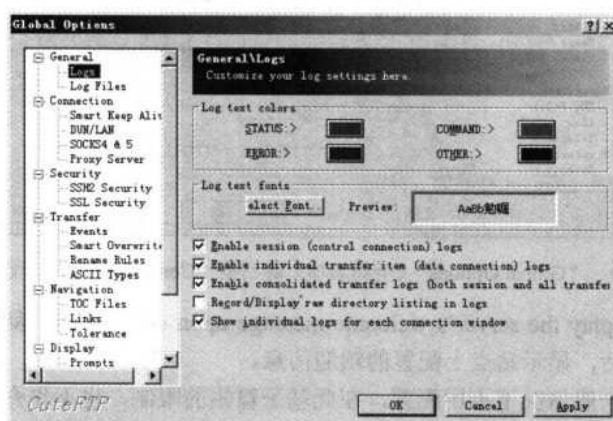


图 4-138 “Global Options”（全局选项）对话框“Logs”选项配置界面

如果选择“Enable session (control connection) logs”复选项，则把每个会话都用一个专门的日志文件记录下来，并在日志窗口中显示每一个会话的日志记录。如果不选择该复选项，则不会用单独的日志文件记录每一个会话连接，当然也就不会在日志窗口中显示每个会话的日志记录。如果选择“Enable individual transfer item (data connection) logs”复选项，则把每个传输项目用一个日志文件记录下来。如果不选择该复选项，则不会用单独的文件记录每一个传输项目。

如果选择“Enable consolidated transfer logs (both session and all transfers in log pane)”复选项，则所有日志以一个日志文件的形式在程序主界面底部的日志窗口统一显示，在一个日志文件中包括了所有活动事件。如果不选择这一复选项，则在日志窗口中不显示日志，也将不用一个日志文件记录所有事件。

250 网管员必读——网络应用（第2版）

如果选择“Record/Display raw directory listing in logs”复选项，则把传输文件列表和用户权限许可也作为会话日志，或者统一日志的一部分记录下来。如果不选择此复选项，则在日志文件中记录文件传输列表和用户权限许可。

如果选择“Show individual logs for each connection window”复选项，则在 CuteFTP 程序主界面右边的远程 FTP 站点窗口中显示连接站点日志窗口。

(3) 在如图 4-138 所示界面左边导航栏中单击“connection”（连接）选项，配置界面如图 4-139 所示。在这里可以设置整个 CuteFTP 程序，以及每个 FTP 站点的最大连接数(Global max 和 Per site max)、连接失败后，允许尝试连接的次数(Connection retry attempts)、两次尝试连接之间的时间间隔(Delay between retries in, 单位为秒)、最长连接时间(Connection timeout in seconds, 单位为秒)、匿名用户电子邮件地址(E-mail address for anonymous)。

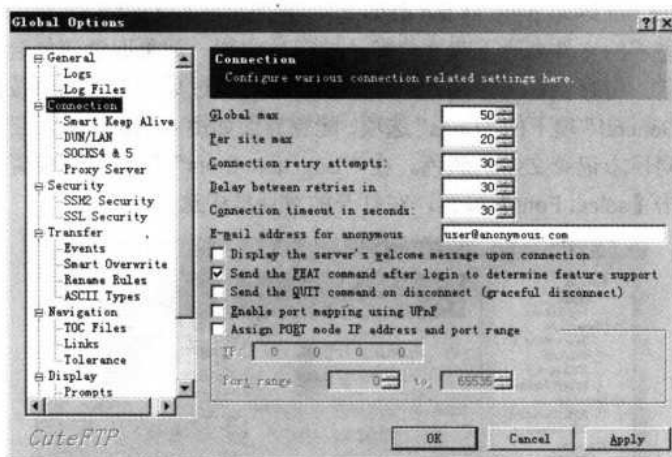


图 4-139 “Global Options”（全局选项）对话框“Connection”选项配置界面

如果选择“Display the server’s welcome message upon connection”复选项，则当用户与 FTP 站点连接成功后，显示站点上配置的欢迎信息。

其他复选项，一般情况下不用配置，在此基于篇幅的限制，也不作介绍。

(4) 在如图 4-139 所示界面左边导航栏中单击“Transfer”（传输）选项，配置界面如图 4-140 所示。在“Transfer”下拉列表中可以选文件传输模式，它有 3 个选项：ASCII、Binary 和 Auto-detect，如果传输的仅是文本文件、网页或其他文档类型文件，则可选择 ASCII 选项；如果所传输的文件中包括图片、图像、程序等非文档文件，则要选择 Binary 选项。通常按默认的“Auto-detect”（自动检测）选择即可。

在“Data mode”（数据模式）下拉列表中有 5 个可选项：PASV、PORT、EPRT、EPSV 和 Auto。对于有些防火墙来说，PASV 是必须选择的，因为客户端需要打开 FTP 服务器端的 IP 地址和端口，选择 PASV 可以避免地址和端口冲突；如果选择 PASV 数据模式时，连接失败，或者发生 socks 协议启动失败，则要选择 PORT（端口）模式；而 EPRT 是一种扩展端口模式，它可以支持 IPv6 协议下的 NAT 类型防火墙；EPSV 是一种扩展 PASV 模式，它同样可支持 IPv6 协议下的 NAT 类型防火墙。通常也可按默认选择 Auto（自动）模式。

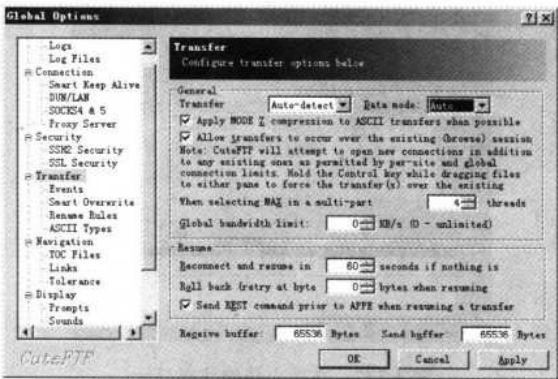


图 4-140 “Global Options”（全局选项）对话框“Transfer”选项配置界面

如果选择了“Apply Mode Z compression to ASCII transfers when possible”复选项，则支持数据压缩模式文件传输，则可节省传输带宽，提高传输性能；如果选择了“Allow transfers to occur over the existing (browse) session”复选项，则允许在已存在会话中启动文件传输进程。

其他选项，一般也无须配置，在此不作介绍。

在如图 4-140 所示配置界面导航栏中的其他选项一般不用特殊配置，为了节省篇幅，在此都不进行介绍。下面主要介绍利用 CuteFTP 进行文件上传和下载的方法。

4.12.4 利用 CuteFTP 进行文件上传和下载

CuteFTP 程序的主要用途就是用来通过网络向 FTP 站点上传文件和下载文件。方法都很简单。上传的文件方法是在如图 4-141 所示界面中选择本地磁盘（Local Driver）上选择要上传的文件或文件夹，单击鼠标右键，在弹出的快捷菜单中选择【Upload】命令即可；如果 CuteFTP 程序中连接了多个 FTP 站点，则可在右键快捷菜单中选择【Upload Advanced】的【Upload to】下的对应 FTP 站点。

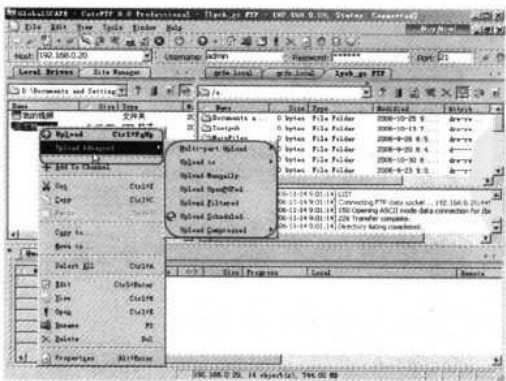


图 4-141 文件上传菜单

开始文件上传后，即在界面底部状态窗口中显示上传进程，完成了上传的项目上会显示一个对号（√）；而正在上传的项目会显示完成情况，如图 4-142 所示。



图 4-142 文件上传的状态显示

从 FTP 站点下载文件的方法是在 CuteFTP 主界面选择相应的 FTP 站点，在中间的详细信息窗口中选择要下载的文件，单击鼠标右键，在弹出的快捷菜单中选择【Download】命令，如果要把下载的文件传输到其他站点中，则可以选择右键快捷菜单中的【Download Advanced】下的【Site to Site Transfer to】下的站点。当然这个站点必须是 CuteFTP 程序已连接的 FTP 站点。参见图 4-143 所示。同样，文件下载完成的项目同样会在状态栏相应下载项目前面打上对号(√)，如图 4-144 所示。



图 4-143 文件下载菜单

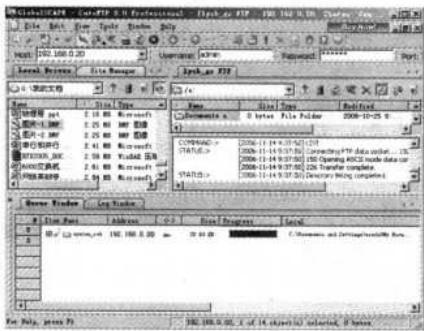


图 4-144 文件下载状态显示

第 5 章 中小型企业邮局系统

企业邮局是目前企业信息化建设的主要目标和应用。随着企业规模的不断扩大，集团公司中各分支机构很可能不在同一城市。有了企业邮局，不仅企业间各员工的通信更加方便，而且因为不必通过外部电子邮件服务商，所以员工之间的邮件通信也更加安全。

企业邮件系统的建设也要根据企业自身的网络规模、经济实力和实际应用需求来选择，如中小型企业通常是选择价格相对便宜（甚至是免费）的低档邮件系统，如 Windows 2000 Server、Windows Server 2003 系统中的 POP3 邮件系统和其他国内一些像 CMail、Winmail 之类的邮件系统。而大中型企业，因为所需的功能更强大，性能更好，建议选择比较大型的邮件系统，如 Microsoft 的 Exchange 2000、Exchange Server 2003 和 IBM 的 Lotus Domino 6 或 7 邮件系统。本章仅介绍适用于中小型企业的 Windows Server 2003 POP3 和 CMail 两种企业邮件系统的建设方法（WindMail 邮件服务器的使用方法与 CMail 基本一样）。下章将介绍适用于大中型企业的 Microsoft Exchange Server 2003 企业邮局方案。Microsoft Exchange 2000 企业邮局方案参见第 1 版的《网管员必读——网络应用》一书。

本章重点

- POP3 邮件系统的组成
- POP3 邮件系统的身份验证方式和特点
- POP3 企业邮局系统基本配置思路
- POP3 和 SMTP 服务器的属性配置
- POP3 邮件系统客户端的配置方法
- CMailServer 邮件服务器的类型和各自的主要应用
- CMailServer 邮件服务器系统的基本配置思路
- CMailServer 邮件服务器的通用设置
- CMailServer 局域网拨号邮件服务器的配置特点
- CMailServer 多域邮件服务器的配置特点
- CMailServer 邮件服务器的客户端设置

5.1 POP3 电子邮件系统概述

电子邮件系统有多种，在小型企业我们完全可直接使用像 Windows 2000 Server、Windows Server 2003 这样的网络操作系统的 POP3 邮件系统。既节约成本（无须另外购买邮件系统软件），又简单、实用。但它只适用于局域网内部使用，不能发送互联网邮件，这一点要特别注意。而本章后面将要介绍的 CMailServer 将可以创建同时应用于局域网和互联网的邮件服务器。

在这样一个完整的邮件系统中，其实包括两个基本的邮件服务，那就是 POP3 和 SMTP 服务，由这两个服务组成虚拟服务器，分别负责邮件的接收和发送。本节先与大家具体了解 POP3 邮件系统的一些基础知识。

5.1.1 POP3 邮件系统的两个基本协议

在 POP3 邮件系统中通常包括 POP3 和 SMTP 两个基本协议，分别负责邮件的接收与发送。它们往往是一起安装与使用的，但如果所配置的邮件服务器仅是用来接收邮件，则可以只配置 POP3 服务；如果仅想用来发送邮件，也可以仅配置 SMTP 协议。

1. POP3 协议

邮局协议 3（POP3）是检索电子邮件的标准协议。它控制着 POP3 电子邮件客户端和存储电子邮件的服务器之间的连接，负责客户端邮件的接收。也就是说，POP3 服务使用 POP3 协议将电子邮件从客户端邮件所在的邮件服务器上检索到 POP3 电子邮件客户端。在邮件服务器上安装 POP3 服务后，用户可以使用支持 POP3 协议的电子邮件客户端（如 Microsoft Outlook）连接到邮件服务器，并将电子邮件检索到本地计算机。POP3 服务与简单邮件传输协议（SMTP）服务一起使用，后者用于发送传出电子邮件。

POP3 协议在处理邮件服务器和 POP3 电子邮件客户端之间的连接时，有以下 3 个过程状态：身份验证状态、事务状态及更新状态。

在身份验证状态下，连接到服务器的 POP3 电子邮件客户端必须先接受身份验证，然后用户才能检索电子邮件。如果电子邮件客户端提供的用户名和密码与服务器上的匹配，则用户通过身份验证，然后进入事务状态。如果不匹配，用户会收到错误消息，不允许连接和检索电子邮件。为防止对邮件存储区的破坏，客户端通过身份验证后，POP3 服务会锁定用户的邮箱。用户通过身份验证后，由于邮箱已被锁定，除非该连接被终止，否则不能下载提交到邮箱的新电子邮件。同样，每次只允许一个客户端连接到邮箱，其他连接邮箱的请求都会被拒绝。

在事务状态下，客户端发送 POP3 命令，同时服务器会根据 POP3 协议接收命令，并做出响应。如果服务器接收的任一客户端请求不符合 POP3 协议，就会被忽略，并返回错误消息。

更新状态是用来关闭客户端与服务器端之间的连接，是客户端发送的最后命令。连接关闭后，邮件存储区会更新，以反映用户连接到邮件服务器后的变化情况。例如，除非用户的电子邮件客户端配置执行其他操作，否则在用户成功检索电子邮件后，已检索的电子邮件将

被标记成删除，然后从邮件存储区中删除。

2. SMTP 协议

简单邮件传输协议（SMTP）控制电子邮件通过 Internet 传送到目标服务器的方式。SMTP 在服务器之间接收和发送电子邮件。在默认情况下，SMTP 服务与 POP3 服务一起安装以便提供完整的电子邮件服务。SMTP 服务自动安装在安装了 POP3 服务的计算机上，从而允许用户发送传出电子邮件。使用 POP3 服务创建一个域时，该域也被添加到 SMTP 服务中（在 IIS 中，具体在本章后面有介绍），以允许该域的邮箱发送传出电子邮件。邮件服务器的 SMTP 服务接收传入电子邮件，并将电子邮件传送到邮件存储区。



当电子邮件无法传送时，简单邮件传输协议（SMTP）服务会将该邮件及一份未送达报告（NDR）返回至发送方。如果 NDR 无法传送到发送方，那么该消息的一份副本会被放入 Badmail 目录。要防止操作系统用完磁盘空间的可能性（如果 Badmail 目录变得非常大），建议将 SMTP Badmail 目录移动至非操作系统卷上。

在 SMTP 协议中，还支持“电子邮件中继”服务。如果用户不是电子邮件域的成员，那么当该用户使用 SMTP 邮件服务器发送电子邮件时，就会发生电子邮件中继。电子邮件中继其实就是一种邮件转发功能，用户可以通过内网的 POP3 邮件系统，借用用户的互联网邮件账户，向外发送电子邮件，收件人看到的只是用户的内网邮件账户，而不显示真正发送邮件时所用的外网邮件账户，正因如此，这一功能被那些想发送大量未经请求的商业电子邮件的人滥用。Microsoft SMTP 服务默认配置为禁止电子邮件中继。

如果要启用电子邮件中继，有以下两种方案，这取决于所使用的身份验证方法。

方案一：如果使用 Active Directory 集成的身份验证，或本地 Windows 账户身份验证，可以配置邮件服务器，要求在接收传出电子邮件之前进行身份验证。如果将 SMTP 服务配置为对尝试发送传出邮件的用户进行身份验证，那么也必须配置用户的电子邮件客户端 SMTP 中继服务，具体将在本章后面介绍。

方案二：如果使用加密码文件，那么要配置电子邮件中继，就必须将邮件服务器配置为允许基于 Internet 协议（IP）地址或电子邮件域名的中继。具体 SMTP 中继配置方法也将在本章后面详细介绍。

5.1.2 电子邮件检索与传输流程

POP3 电子邮件系统的邮件传输与检索流程如图 5-1 所示（在此，仅以互联网电子邮件为例，企业内部邮件的发送与接收原理一样，只不过此时的邮件服务提供商就是本单位的邮件服务器）。该图阐释了电子邮件是如何从发件人传送到收件人，以及如何检索到收件人的本地计算机上的。

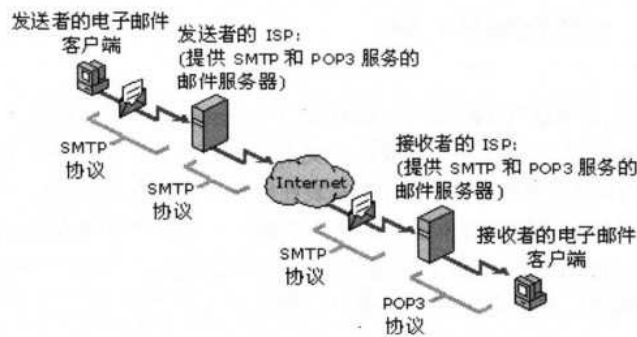


图 5-1 电子邮件的传输与检索流程

发件人的客户端计算机通过 Internet 服务提供商（ISP）连接到 Internet。发件人使用电子邮件客户端发送电子邮件。根据 SMTP 协议，电子邮件被提取，再传送到发件人的 ISP，然后由该 ISP 路由到 Internet 上。

电子邮件在 Internet 上，经过许多中间服务器中继，才传送到收件人。当电子邮件到达收件人的 ISP 时，就被放入收件人的邮箱。当收件人的计算机连接到他的 ISP 时，根据 POP3 协议，电子邮件就从该 ISP 传送到收件人本地计算机的电子邮件客户端上。

5.1.3 POP3 电子邮件系统的组件

POP3 电子邮件系统由以下 3 个组件组成：POP3 电子邮件客户端、SMTP 服务和 POP3 服务。各组件的功能描述如表 5-1 所示。

表 5-1 POP3 邮件组件

组 件	描 述
POP3 电子邮件客户端	POP3 电子邮件客户端是用于读取、撰写及管理电子邮件的软件。POP3 电子邮件客户端从邮件服务器检索电子邮件，并将其传送到用户的本地计算机上，然后由用户进行管理。例如，Outlook Express 就是一种支持 POP3 协议的电子邮件客户端
SMTP 服务	SMTP 服务是使用 SMTP 协议将电子邮件从发件人路由到收件人的电子邮件传输系统。POP3 服务使用 SMTP 服务作为电子邮件传输系统。用户在 POP3 电子邮件客户端撰写电子邮件。然后，当用户通过 Internet 或内部网络连接来连接邮件服务器时，SMTP 服务将提取电子邮件，并通过 Internet 将其传送到收件人的邮件服务器
POP3 服务	POP3 服务是使用 POP3 协议将电子邮件从邮件服务器上下载到用户本地计算机上的电子邮件检索系统。用户的 POP3 电子邮件客户端和存储电子邮件的服务器之间的连接，是由 POP3 协议控制的

管理员可在以下 3 种组织级别上管理 POP3 服务：邮件服务器、电子邮件域及邮箱。如表 5-2 所示。

表 5-2 管理员可以管理的选项

分 类	描 述
邮件服务器	邮件服务器是安装 POP3 服务的计算机。用户可以连接到邮件服务器来检索电子邮件

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(续表)

分 类	描 述
电子邮件域	电子邮件域必须是已注册的域名（可以是内、外部域名），并且该域名必须与 Internet 服务提供商（ISP），或者企业内部网络域所创建的邮件交换器（MX）记录相匹配
邮箱	每个邮箱对应一个用户，该用户是电子邮件域的成员，如 someone@example.com。用户的邮箱对应邮件存储区的一个目录，该目录用于在用户检索电子邮件之前存储这些电子邮件

如图 5-2 所示，是一个互联网 POP3 电子邮件系统中客户端邮件发送和接收的基本流程（各步骤在图中已有标识）。

- （1）某用户发送一封目的地址为 someone@example.com 的电子邮件发送到他的邮件服务提供商，或者本地网络的邮件服务器所在域 example.com 上。
- （2）example.com 域上的邮件服务器收到客户端发来的邮件后，由 SMTP 服务提取该电子邮件，并将其发送到 Internet。
- （3）通过互联网上的相应 DNS 服务器将电子邮件域（example.com）解析成 Internet 上的邮件服务器（假设为 mailserver1.example.com）。mailserver1.example.com 是运行 POP3 服务的邮件服务器，该服务器为电子邮件域 example.com 接收传入的电子邮件。
- （4）mailserver1.example.com 邮件服务器接收这封由某用户发来的 someone@example.com 客户端电子邮件。

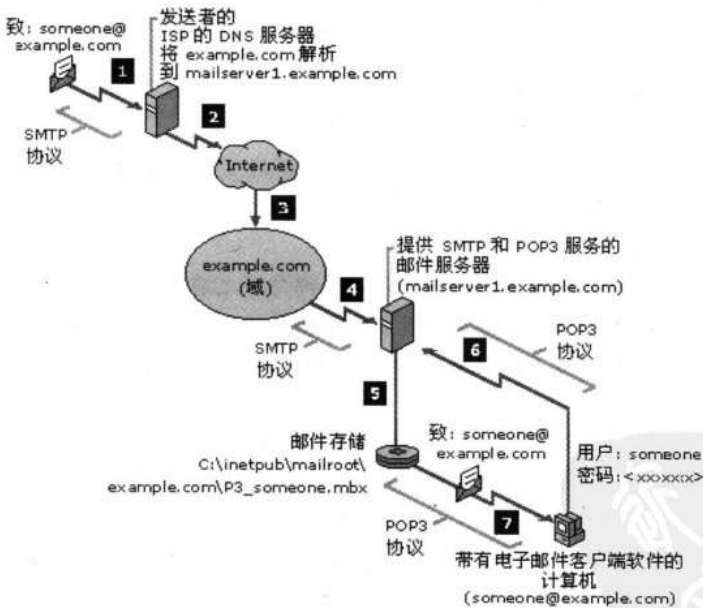


图 5-2 POP3 电子邮件系统邮件发送、接收流程

- （5）mailserver1.example.com 邮件服务器把 someone@example.com 客户端电子邮件转到邮件存储目录中，该目录用于存储 someone 客户的电子邮件（不同客户有不同目录）。
- （6）用户“someone”客户端连接到运行 POP3 服务的邮件服务器来检查电子邮件。POP3 协议传输用户“someone”的用户和密码身份验证凭据。POP3 服务验证这些凭据，然后决定

接受或拒绝该连接。

（7）如果连接成功，用户“someone”所有的电子邮件（存储在邮件存储区），将从邮件服务器下载到该用户的本地计算机上。然后，通常该邮件会从邮件存储区删除。



POP3 和 SMTP 协议是不加密的协议。如果有人获得运行 POP3 服务的服务器所在网络的访问权限，就有可能读取用户的电子邮件。要提高网络的安全性，可以实施 Internet 协议安全性（IPSec）。IPSec 是一种用于保护私人秘密的开放标准的框架结构，通过使用加密安全服务来确保 Internet 协议（IP）网络上的安全通信。具体的 IPSec 协议介绍将在本系列《网管员必读——网络安全》一书中介绍。

5.1.4 POP3 服务身份验证

为了确保接收邮件的人是真实的用户，POP3 服务必须提供相应的用户身份验证方法。在 POP3 服务中，提供了 3 种不同的身份验证方法来验证连接到邮件服务器的用户。表 5-3 描述了这 3 种身份验证方法的使用方法。

表 5-3 POP3 的 3 种身份验证方法

身份验证方法	何时使用该身份验证方法
本地 Windows 账户身份验证	如果邮件服务器不是 Active Directory 域的成员；并且要在安装了 POP3 服务的服务器上存储用户账户时就选择此身份验证方案
Active Directory 集成的身份验证	如果邮件服务器是域控制器，或者是 Active Directory 域的成员时选择使用此身份验证方案
加密码文件身份验证	如果邮件服务器没有使用 Active Directory 域；或不希望本地计算机上存在 POP3 服务的用户账户时选择此身份验证方案



在邮件服务器上创建任何电子邮件域之前，必须选择一种身份验证方法。而且只有在邮件服务器上没有电子邮件域时，才可以更改身份验证方法，在创建了邮件域后不能更改身份验证方法。



如果运行 POP3 服务的计算机是 Active Directory 域的成员或是域控制器，以上 3 种身份验证方法均可用，但默认的身份验证方法是 Active Directory 集成的身份验证。否则，默认使用本地 Windows 账户身份验证。如果运行 POP3 服务的计算机是域控制器，则可用的身份验证方法是 Active Directory 集成的身份验证和加密码文件身份验证。如果不是以上两种情况，则可用的身份验证方法为本地 Windows 账户身份验证和加密码文件身份验证。

1. 本地 Windows 账户身份验证

如果不使用 Active Directory（也就是说邮件服务器既不是域控制器，也不是域成员服务器），但又想在安装了 POP3 服务的本地计算机上创建用户账户，那么，可以使用本地 Windows 账户身份验证将 POP3 服务和本地系统用户账户联系起来。当邮件服务器不是 Active Directory 域的成员，并且希望在安装了 POP3 服务的本地计算机上也拥有用户账户时，可使用本地

Windows 账户身份验证方式。

本地 Windows 账户身份验证将 POP3 服务集成到本地计算机的安全账户管理器（SAM）中。通过使用安全账户管理器，在本地计算机上拥有用户账户的用户，就可使用由 POP3 服务或本地计算机进行身份验证的相同的用户名和密码。



本地 Windows 账户身份验证可以支持服务器上的多个域，但是不同域上的用户名必须唯一。例如，用户名为 `someone@example.com` 和 `someone@northwindtraders.com` 的用户不能同时存在，前面的用户名一定要不相同。

2. Active Directory 集成的身份验证

当要安装 POP3 服务的服务器是 Active Directory 域的成员或者是 Active Directory 域控制器时，可以使用 Active Directory 集成的身份验证方式。可以使用 Active Directory 集成的身份验证将 POP3 服务集成到现有的 Active Directory 域中。如果创建的邮箱与现有的 Active Directory 用户账户相应，用户就可以使用现有的 Active Directory 域用户名和密码来收发电子邮件。

如果使用 Active Directory 集成的身份验证，并且有多个 POP3 电子邮件域，那么在创建邮箱时，请确保新邮箱的名称与其他 POP3 电子邮件域中现有邮箱的名称不同。每个邮箱与一个 Active Directory 用户账户对应，该账户同时拥有完全域名用户登录名和 Windows 2000 以前系统版本的 NetBIOS 用户登录名。



可以使用 Active Directory 集成的身份验证来支持多个 POP3 电子邮件域，这样就可以在不同的 POP3 电子邮件域上使用相同的用户名。例如，可以使用名为 `someone@example.com` 的用户和名为 `someone@northwindtraders.com` 的用户。然而，当存在 Windows 2000 混合域模式中创建用户登录名相同的用户账户时将会导致命名冲突。Active Directory 不支持具有 Windows 2000 以前版本的同一用户登录名的多个账户。如果发生命名冲突，邮箱名和电子邮件地址不会受到影响，但是该账户的 Windows 2000 以前版本的邮箱登录名会被修改，从而防止与现有的账户发生任何命名冲突。具体在本章后面的小节中介绍。

3. 加密密码文件身份验证

加密密码文件身份验证方式是在没有使用 Active Directory 域，或不想在本地计算机上创建用户时使用。加密密码文件身份验证对于还没有部署 Active Directory 的大规模部署十分理想，并且从一台本地计算机上就可以很轻松地管理可能存在的大量账户。

使用加密密码文件身份验证，可以在不同的邮件域中使用相同的用户名。但是，不能在一个域中将同一用户名指派给多个邮箱。例如，不能有两个名为 `someone@example.com` 的邮箱，但可以使用 `someone@example.com` 和 `someone@northwindtraders.com`。

加密密码文件身份验证使用用户的密码创建一个加密文件，该文件存储在服务器上用户邮箱的目录中。在身份验证过程中，用户提供的密码被加密，然后与存储在服务器上的加密文件比较。如果加密的密码与存储在服务器上的加密密码匹配，则用户通过身份验证。

可以使用 `winpop.exe` 命令行工具将加密密码文件身份验证下创建的用户账户，迁移到 Active Directory 用户账户中。

5.1.5 邮件存储区

邮件存储区其实就是一个用来存放客户端邮件的目录，用于 POP3 服务存储所有的电子邮件，直到用户将其检索到客户端计算机（也可能用户检索后仍保留副本）。

邮件存储区（根邮件目录）的基本结构是本地硬盘上存储所有电子邮件的目录。创建域时，POP3 服务将在为邮件存储区指派的目录下创建相应的目录。在邮件域目录中，POP3 为域中每个拥有邮箱的用户创建一个目录（也就是用户邮箱），用户收到的电子邮件以单个文件的形式存放在相应用户的目录中，直到用户用 POP3 电子邮件客户端检索该邮件。

例如，下面是邮件存储区中一封电子邮件的路径：

C: \inetpub\mailroot\mailbox\example.com\P3_someone.mbx\P347865.eml

此处，mailroot 对应邮件存储目录，example.com 对应邮件域目录，P3_somone.mbx 对应邮箱名为 someone 的目录，P347865.eml 对应保存的单个电子邮件。

邮件存储区的每个目录有相同的目录结构和文件权限。当配置邮件存储区时，仅为本地或域管理员及本地网络服务（用于运行 POP3 服务）指派访问该目录的权限，而不为其他用户指派读取/更改权限。

邮件存储区的功能取决于是否拥有足够的可用硬盘空间。为确保邮件存储区的正常使用，应该根据服务器上用户的数量、用户接收电子邮件的数量以及接收的电子邮件的平均大小，对所需的磁盘空间进行估算。然后，再使用磁盘配额，防止在服务器上出现邮件存储区的磁盘使用意外增长的情况（因为配置后，超出限制可以报警提醒）。磁盘配额可以监视和控制 NTFS 文件系统卷上的磁盘空间。

因为邮件存储可能会潜在地使用大量磁盘空间，所以，应该在邮件存储所在的卷上设置磁盘配额限制（以便控制磁盘空间使用率）或设置邮件存储不使用操作系统所在的卷。如果邮件存储变得非常大，这将防止操作系统用完磁盘空间的可能性。有关用户邮箱的磁盘配额配置也将在本章后面介绍。



必须使用本地硬盘的目录或 UNC 路径来配置邮件存储区；不支持其他存储选项，例如，映射驱动器。不能将邮件存储区设置成硬盘的根目录（例如 C:\），或当前正在使用的目录。

要从备份中恢复邮件存储区，或者将其转到新的位置，必须使用命令程序重新设置邮件存储区目录的权限；要将邮件存储区转到新的目录，那么在移动邮件存储区时，必须确保该目录保留正确的所有权；复制邮件存储区不起作用。

到服务器的物理访问存在很高的安全风险，要维持更高的安全环境，可以限制对邮件存储区所在服务器的物理访问。

5.1.6 POP3 邮件系统建设基本思路

本节同样要先向大家介绍一下 POP3 邮件系统建设的基本思路，按照这个思路就可以比较顺利地架设自己企业的小型邮件系统。

利用 Windows Server 2003 R2 系统（其他版本系统的建设方法也类似）的邮件系统建设

基本思路如下。

1) 安装 POP3 邮件系统组件

这也是必须的前提，在 Windows Server 2003 R2 系统中安装 POP3 邮件系统组件的方法有两种：一是利用“配置你的服务器向导”进行；二是利用控制面板中的“添加或删除程序”工具进行。

具体安装步骤参见 5.2 节。

2) POP3 邮件系统的基本属性配置

安装了 POP3 邮件系统后需要对 POP3 和 SMTP 两服务器进行必要的基本属性配置，主要是 SMTP 服务器的配置。其中就包括用于存放 POP3 接收邮件的目录，SMTP 服务器的 IP 地址、端口号、身份验证方法、连接控制、中继连接限制，以及邮件附件大小、会话大小和每个连接的邮件数等。还可以配置 SMTP 服务器操作员账户。

具体配置方法参见 5.3 节。

3) POP3 邮件系统的高级配置

因为 POP3 邮件系统是一个简单的内部局域网邮件系统，它不具备用户邮箱大小配置功能，需要借助于 Windows 系统中的磁盘配额功能来实现。另外，还需要为用户发送邮件选择一种具体的身份验证方式。具体参见 5.4 节的介绍。

4) POP3 客户系统配置

POP3 邮件系统的客户系统配置包括用户账户的创建与配置，以及客户端邮件接收系统的配置两个方面。具体配置方法参见 5.5 节。

5.2 安装邮件服务器

本节仅以在 Windows Server 2003 R2 域网络中安装 POP3 邮件系统，并以 Active Directory 身份验证方式为例进行介绍，这也是目前企业应用最普遍的一种邮件系统部署方法。

在 Windows Server 2003 系统中，邮件服务器的安装有两种可行的方式：一种是所有服务器安装的通用方式，即“配置你的服务器向导”法；另一种就是利用系统的“添加或删除程序”控制面板工具。虽然在“配置你的服务器向导”法安装中也没有太多具体配置，但它却可以配置邮件域，而在采用“添加或删除程序”工具安装 POP3、SMTP 服务组件的方法中不能配置邮件域，需要在组件安装后，再在 POP3 控制台中创建。下面对以上两种方法分别予以介绍。

5.2.1 利用“配置你的服务器向导”进行安装

这种方法在《网管员必读——网络组建》一书中介绍像域控制器、DNS、DHCP、WINS 服务器安装时用得最多了，所以说它是一种服务器通用安装方式。

(1) 执行【开始】→【管理工具】→【配置您的服务器向导】菜单操作，打开如图 5-3 所示的向导首页对话框。



从这里可以看出，虽然表面上看来，此处所安装的仅是 POP3 邮件服务器，但实际上是同时安装了 POP3 和 SMTP 服务。只不过安装后，这两个服务不是一起的，而分属于不同的控制台来配置，POP3 服务是在安装后添加的 POP3 管理工具控制台中配置，而 SMTP 则是在 IIS 中配置的。具体将在本章后面介绍。

(4) 单击【下一步】按钮，打开如图 5-6 所示的对话框。在其中要求选择邮件服务器中所使用的用户身份验证方法，这就要根据本章前面所介绍的 POP3 身份验证方法选择原则来进行。如果是在域网络的域控制器，或者成员服务器上安装，则可以选择“Active Directory 集成的”，或者“加密的密码文件”两种方式之一；如果是在没有域的网络中进行安装，则有“本地 Windows 账户身份验证”和“加密的密码文件”两种方式选择。具体选择哪种要根据实际需要选择，参见本章前面 5.1.4 中的介绍。本示例因为是在域网络中，并且想利用域用户账户进行身份认证，所以选择“Active Directory 集成的”这种方式。

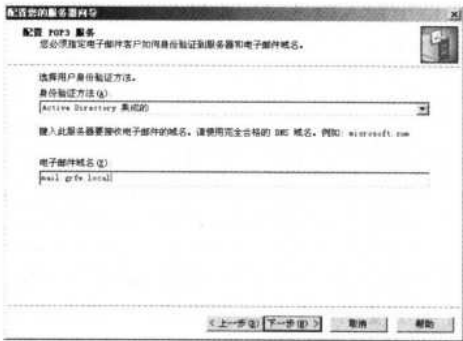


图 5-6 “配置 POP3 服务”对话框

在“电子邮件域名”文本框中输入该邮件服务器域名。此处的“电子邮件域名”不一定要与当前网络域的域名一样，POP3 服务支持顶级和三级域名。例如“.”（根域）、“example.com”和“mailserver.example.com”都是受支持的。本示例为 mail.grfw.local。



如果所配置的邮件系统域名与当前网络域名不一样（特别是创建用来收发互联网等外部邮件的 POP3 邮件系统），则需在当前网络的 DNS 服务器创建一条指向该邮件域邮件交换器主机的 MX 邮件交换记录。MX 记录为发送到该域名的电子邮件提供到邮件交换器主机的电子邮件路由。例如，本例中，在网络域为 grfw.local 中，而此处所创建的邮件服务器域名为 mail.grfw.local。于是我们就得在 grfw.local 域的 DNS 服务器上创建一个指向 mail.grfw.local 的 MX 记录。这样，发送到 someone@grfw.local 的电子邮件将被路由到 mail.grfw.local 主机下。

MX 记录的配置方法很简单，具体操作如下。

在 DNS 服务器计算机上打开 DNS 控制台，找到对应的查找区域（一般为网络域名，DNS 安装后会自动创建，如图 5-7 所示的 grfw.local），单击鼠标右键，在弹出的快捷菜单中选择【新建邮件交换器（MX）】命令，打开如图 5-8 所示的对话框。



图 5-7 DNS 服务器控制台

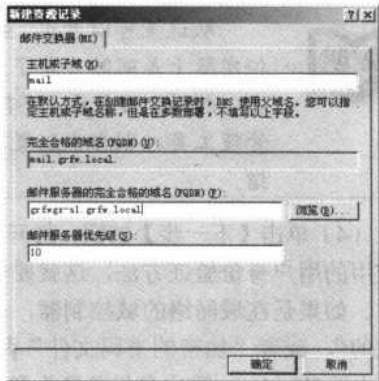


图 5-8 “新建资源记录”对话框“邮件交换器 (MX)”选项卡

在“主机或子域”文本框中输入该区域中邮件交换器的单一部分名称，如设定的邮件域为 mail.grfw.local，则此处的单一部分名称就为 mail。如果将其保留为空，则邮件交换器名与父域名相同（在邮件域与当前网络域名完全一样时）。如果需要在此处添加包含句点（.）的名称以指明额外域等级的名称，则首先在 DNS 控制台中分别地添加其他域，然后添加作为单一部分名称的新 MX 记录。如新的邮件域名称为 mail.sales.grfw.local，则先需在 DNS 中创建这样一个查找区域，然后再在这个区域中打开如图 5-8 所示的对话框，不过此时在“主机或子域”栏中就要输入 mail.sales。下面的“完全合格的域名（FQDN）”文本框会自动显示所配置的邮件域名。在“邮件服务器的完全合格的域名（FQDN）”文本框中输入该邮件服务器的完全合格的域名，或者单击【浏览】按钮在网络中定位查找。

在“邮件服务器优先级”文本框中键入一个 0~65 535 之间的数值，该值指明相对于其他邮件交换服务器的邮件交换服务器的优先级。将较低数值的首选项授予 MX 资源记录中引用的具有较高优先级数的服务器。使用零值（0）时，系统将授予邮件交换服务器最高的优先级或首选项。在出现多个 MX 资源记录时，邮件程序首先试图用最低的首选项值传递到邮件交换服务器中。如果传递失败，则尝试使用带有下一个最高首选项值的邮件交换服务器。如果有两个或多个邮件交换服务器共享同一个首选项值，则该邮件程序会尝试随机地使用某个类似的值。

（5）单击【下一步】按钮，打开如图 5-9 所示的对话框。这是一个选择总结对话框，在列表中总结了以上配置选择，只是用于再次确认，无须任何具体的配置。



图 5-9 “选择总结”对话框

(6) 单击【下一步】按钮后，系统开始安装邮件服务器所需的组件，进程如图 5-10 所示。不过在此过程中，系统会提示用户指定 Windows Server 2003 系统源程序所在位置，以便复制所需文件。

(7) 完成文件复制后系统会自动打开如图 5-11 所示向导完成对话框。直接单击【完成】按钮完成邮件服务器的整个安装过程。完成后执行【开始】→【管理工具】→【管理你的服务器】菜单操作，在打开的如图 5-12 所示“管理你的服务器”窗口即可见到刚才安装的邮件服务器了。单击【管理此邮件服务器】按钮即可打开邮件服务器窗口，如图 5-13 所示。

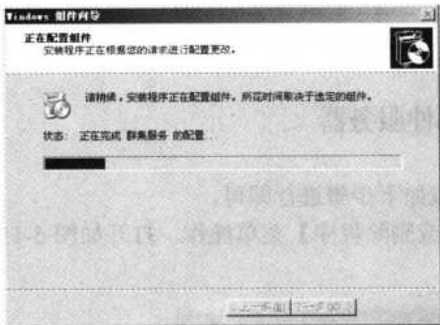


图 5-10 “正在配置组件”对话框

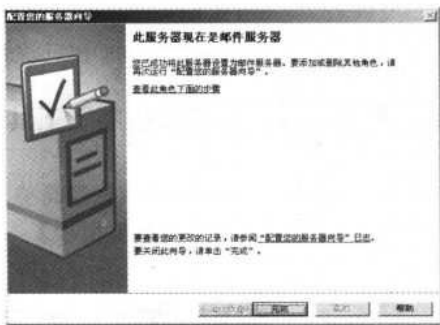


图 5-11 “此服务器现在是邮件服务器”对话框

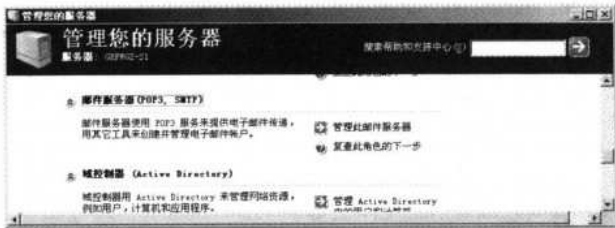


图 5-12 “管理你的服务器”窗口

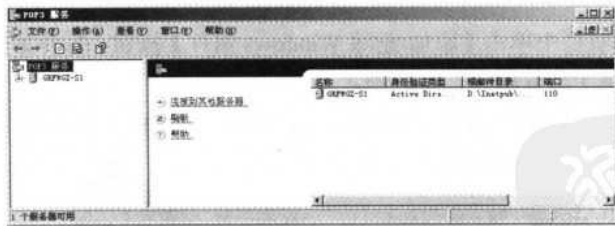


图 5-13 “POP3 服务”窗口

除了在【管理工具】程序菜单中添加了【POP3 服务】这个管理工具外，还在 IIS 的“默认 SMTP 虚拟服务器”选项上添加了新的邮件服务器域，如图 5-14 所示。



图 5-14 在 IIS 中添加的邮件服务器域的 SMTP 虚拟服务器

5.2.2 利用“添加或删除程序”工具安装邮件服务器

这种方式的邮件服务器安装相当简单，只需按如下步骤进行即可。

(1) 执行【开始】→【控制面板】→【添加或删除程序】菜单操作，打开如图 5-15 所示的对话框。



图 5-15 “添加或删除程序”对话框

(2) 在左边导航栏中单击【添加/删除 Windows 组件】按钮，打开如图 5-16 所示的对话框。在其中选择“电子邮件服务”复选项。

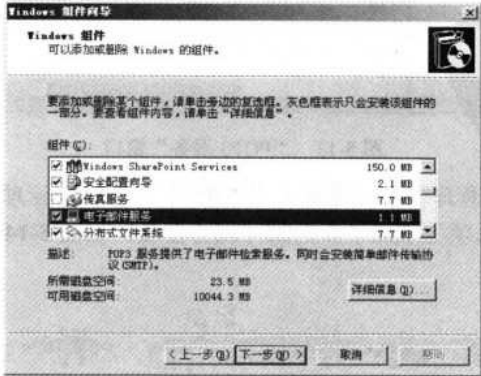


图 5-16 “Windows 组件向导”对话框

(3) 单击【详细信息】按钮，打开如图 5-17 所示的对话框。其中的两个复选项可根据需要选择，但至少应该选择“POP3 服务”选项，至于“POP3 服务 Web 管理”选项是否选择，则要根据是否需要通过 Web 方式对邮件服务器进行管理来决定了。通常为了管理上的方便，选择该选项，以便管理员不在服务器旁边时，通过其他任何计算机远程管理该邮件服务器。

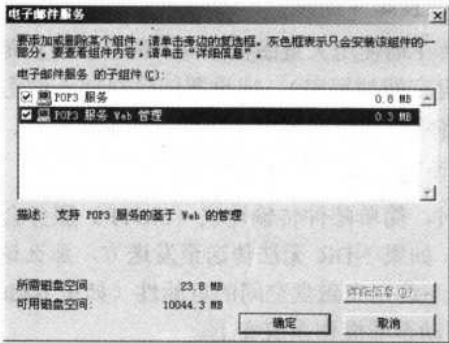


图 5-17 “电子邮件服务”对话框



在前面的“配置你的服务器向导”安装法中所安装的邮件服务器中是没有安装“POP3 服务 Web 管理”选项的，也就是所安装的邮件服务器默认不具有 Web 管理功能。

(4) 单击【确定】按钮，回到如图 5-16 所示的对话框。然后单击【下一步】按钮，系统会自动安装所需组件，在复制文件的时候也要提供 Windows Server 2003 系统源程序位置。完成后执行【开始】→【管理工具】→【POP3 服务】菜单操作，同样会打开如图 5-13 所示的“POP3 服务”窗口。不过，用此方法添加的 POP3 邮件系统，在初次打开 POP3 窗口时，是不能见到任何邮件域的，需要先添加域，这就是与使用“配置你的服务器向导”方法创建的不同之处。

添加邮件域的方法很简单，只需在如图 5-13 所示控制台窗口中单击“新域”链接，即可打开如图 5-18 所示的对话框，在其中输入邮件域名称，单击【确定】按钮即可。同样如果输入的邮件域与当前网络域名不一样，则需要事先在 DNS 服务器上创建 MX 邮件交换器记录，参见前面的介绍。邮件域创建好后才能进行其他操作与配置，如创建用户邮箱等。

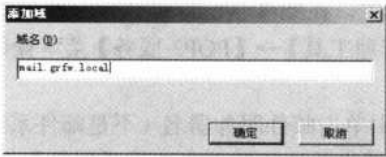


图 5-18 “添加域”对话框

5.3 POP3 邮件服务器配置

上节我们安装好了 POP3 系统邮件服务器，本节首先要介绍的是这个新邮件系统中的邮件服务器（包括接收邮件服务器 POP3 服务器和发送邮件服务器 SMTP 服务器）配置。下面

先来了解一下有关 POP3 和 SMTP 邮件服务器配置的参考建议。

5.3.1 邮件服务器配置参考建议

1. 在非操作系统卷上设置邮件存储

因为邮件存储可能会潜在地使用大量磁盘空间，所以应该在邮件存储所在的卷上设置磁盘配额限制（以便控制磁盘空间使用率），或设置邮件存储不使用操作系统所在的卷。如果邮件存储变得非常大，这将防止操作系统用完磁盘空间的可能性。

2. 在非操作系统卷上设置 Badmail（死信）目录

当电子邮件无法传送时，简单邮件传输协议（SMTP）服务会将该邮件及一份未送达报告（NDR）返回至发送方。如果 NDR 无法传送到发送方，那么该消息的一份副本会被放入 Badmail 目录。要防止操作系统用完磁盘空间的可能性（如果 Badmail 目录变得非常大），必须将 SMTP Badmail 目录移动至非操作系统卷上。

3. 使用 NTFS 文件系统的分区作为邮件存储区，并且实施磁盘配额

NTFS 文件系统的分区提供了较安全的目录和文件夹。这样可以增强对存储在本地硬盘上的电子邮件的保护。

磁盘配额可以防止邮件存储区使用过多的或无法预计的磁盘空间。使用过多的或无法预计的磁盘空间可能对运行 POP3 服务的服务器的性能产生不利影响。因此，这样做十分重要。

4. 为邮件存储区分配足够的磁盘空间

为确保给邮件存储区分配足够的磁盘空间，可以根据服务器上的用户数、用户接收电子邮件的数量以及接收电子邮件的平均大小，来估计所需的磁盘空间。

5. 使用加强的密码保护邮件服务器

加强密码可以防止对邮件服务器的非授权访问。

5.3.2 POP3 服务器属性配置

邮件服务器的配置包括两方面：POP3 服务器属性配置、SMTP 虚拟服务器配置。本节首先介绍 POP3 服务器属性配置，在此以 Windows Server 2003 R2 系统为例。

（1）执行【开始】→【管理工具】→【POP3 服务】菜单操作，打开如图 5-13 所示 POP3 邮件服务器窗口。

（2）在窗口左边导航栏中单击邮件服务器名（不是邮件系统域名，本示例为 GRFWGZ-S1），然后单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，或者在右边详细信息窗口中单击“服务器属性”链接（必须要在左边导航栏中选择了相应的邮件服务器，在右边详细信息窗口中才有该链接出现），都可打开如图 5-19 所示 POP3 邮件服务器属性对话框。从中可以看出，POP3 服务器的配置非常简单。

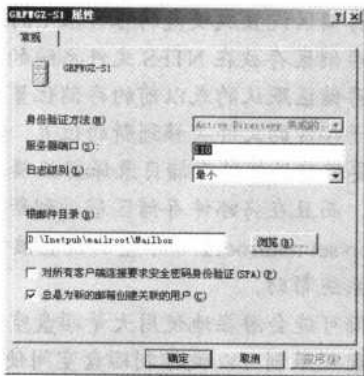


图 5-19 POP3 邮件服务器属性对话框

在这个对话框中除了安装时所选择的身份验证方法不可重新配置外（本章前面已有说明，身份验证方式在邮件域添加后是不可改变的），其他都可以。但“服务器端口”栏中的设置不要更改，因为这是系统默认的端口，也是公认的 POP3 服务所用端口。

在“日志级别”下拉列表中有 4 种日志级别选择，如果选择“无”选项，则不记录 POP3 服务事件；如果选择“最小”选项，则记录 POP3 服务关键事件；如果选择“中”选项，则记录 POP3 服务关键和警告事件；如果选择“最大”选项，则记录 POP3 服务关键、警告和信息事件。



注意

如果更改该参数，则必须停止并重新启动 POP3 服务和 IIS 管理服务。如果你正在使用 Active Directory 集成的身份验证，则必须登录到 Active Directory 域（而不是本地计算机）才能执行此过程。

在“根邮件目录”栏中，可以配置邮件服务器用来存储客户端邮件的目录，在此要键入邮件存储区的路径。系统默认路径为系统区下的 \inetpub\mailroot\Mailbox，最好不要改，这样更便于对所有应用服务器的管理。不过，要注意，这个路径的最大值为 260 个字符。邮件存储区必须是一个本地文件系统的目录，或者是通用命名约定（UNC）路径，也就是网络共享路径，不支持磁盘映射。可单击【浏览】按钮，打开如图 5-20 所示的对话框，在其中就可以选择本地，或者网络存储路径。



图 5-20 “浏览文件夹”对话框



不能将邮件存储区设置成硬盘的根目录（例如 C: \）或文件正在使用的目录。建议将邮件存储区存放在 NTFS 文件系统的分区上。

要更改邮件存储区默认的或以前的存储位置，并且已存储电子邮件，则必须手动将存放电子邮件的文件夹移到新的位置。如果将邮件存储区移动到新的目录，必须确保要移动的邮件存储目录保留正确的所有权；仅通过复制邮件存储区做不到这点。而且在将邮件存储区移动到新的位置或者从备份中恢复后，必须使用【winpop set mailroot】命令重新设置该目录的权限。这一命令的详细使用方法请参见系统帮助。

因为邮件存储可能会潜在地使用大量磁盘空间，所以应该在邮件存储所在的卷上设置磁盘配额限制（以便控制磁盘空间使用率），或设置邮件存储不使用操作系统所在的卷。如果邮件存储变得非常大，这将防止操作系统用完磁盘空间的可能性。有关磁盘配额方面的知识在本系列丛书《网管员必读——网络管理》一书中介绍。

如果选择了“对所有客户端连接要求安全密码身份验证（SPA）”复选项，则要求连接到该 POP3 服务器的所有电子邮件客户端进行安全身份验证，具体将在本章后面介绍邮件系统客户端配置时介绍。

如果选择了“总是为新的邮箱创建关联的用户”复选项，则在 POP3 服务器中创建了新邮箱时自动创建与在 Active Directory 或本地计算机中的邮箱名相对应的用户。系统默认选择此复选项，否则创建用户邮箱就没有意义了，因为此处采用的是与 Active Directory 集成的身份验证方式。

5.3.3 SMTP 虚拟服务器属性配置

SMTP 服务器的属性配置分两个方面进行，一是就整体系统中的 IIS SMTP 服务器进行的，另一个则是针对具体的邮件域 SMTP 服务进行的。下面分别予以介绍。

1. 默认 SMTP 虚拟服务器属性配置

下面首先介绍整体系统中的 SMTP 服务器属性配置。具体步骤如下。

（1）执行【开始】→【管理工具】→【Internet 信息服务（IIS）管理器】菜单操作，打开如图 5-14 所示“Internet 信息服务（IIS）管理器”控制台窗口。

（2）在左边导航栏中单击本地服务器前面的“+”号，展开各选项，然后选择“默认 SMTP 虚拟服务器”选项，单击鼠标右键，在弹出的快捷菜单中单击【属性】命令，打开如图 5-21 所示的对话框。在这里可以设置默认 SMTP 虚拟服务器的 IP 地址、限制连接数，连接超时、是否启用日志记录及日志记录的格式等选项。在“IP 地址”栏后面单击【高级】按钮，打开如图 5-22 所示的对话框。与本书前面介绍的 Web 网站和 FTP 站点类似，在这里也可以添加新的 SMTP 服务器标识，或者编辑现有标识。SMTP 服务器标识是由 IP 地址和所用端口共同决定的，但通常所用的 25 号端口是不能改变的，所有只能通过不同的 IP 地址来标识不同的 SMTP 服务器。要新建 SMTP 标识，只需单击【添加】按钮，打开如图 5-23 所示的对话框，在这里就可以配置 IP 地址和所用的端口了。



图 5-21 “默认 SMTP 虚拟服务器属性”对话框
“常规”选项卡

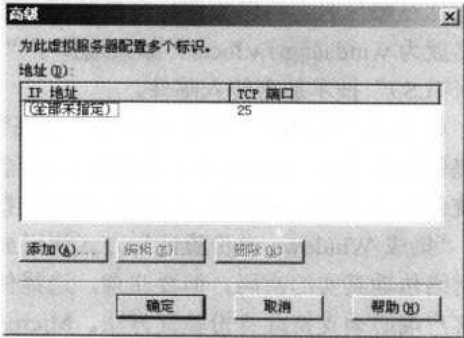


图 5-22 “高级”对话框

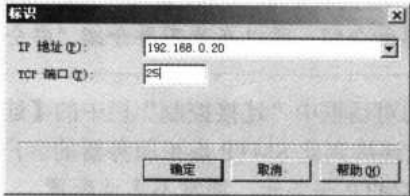


图 5-23 “标识”对话框

(3) 选择“访问”选项卡，如图 5-24 所示。这里的配置就比较复杂了。首先单击“访问控制”栏中的【身份验证】按钮，打开如图 5-25 所示的对话框。

如果选择了“匿名访问”复选项，则允许所有客户端无须用户名和密码地通过访问 SMTP 服务器向外发送邮件。通过选中此选项并清除其余两个选项，可以禁用该虚拟服务器上的其他身份验证。但通常出于安全考虑，不这样配置。



图 5-24 “默认 SMTP 虚拟服务器属性”
对话框“访问”选项卡

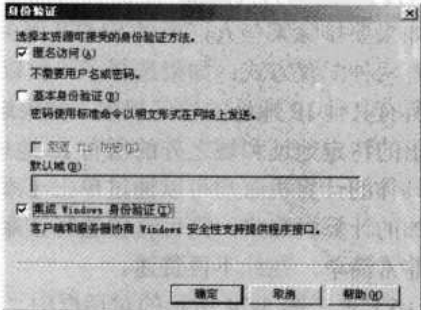


图 5-25 “身份验证”对话框

272 网管员必读——网络应用（第2版）

如果选择“基本身份验证”复选项，则可以启用“基本（明文）”密码验证。对于基本身份验证，账户名和密码将以明文形式传输。另外，还需要在“默认域”文本框中指定一个域附加在账户名之后以便进行身份验证，如域为 grfw.local，用户名为 winda，则完整的用户名就为 winda@grfw.local。如果选择了“需要 TLS 加密”复选项，则要求使用“传输层安全（TLS）”技术加密传入邮件。

如果选择了“集成 Windows 身份验证”复选项，则会启用 Microsoft .NET Server 系列产品提供的标准安全机制。这种安全机制使企业为用户提供安全登录服务成为可能。已在内部系统使用“集成 Windows 身份验证”的虚拟服务器可以通过使用单一、公共的安全机制而受益。“集成 Windows 身份验证”方式使用加密技术对用户进行身份验证，并且不要求用户通过网络传输真实的密码。但要注意，选择使用“集成 Windows 身份验证”方式，则要求邮件客户端必须支持此身份验证方法。Microsoft Outlook Express 客户端支持“集成 Windows 身份验证”方式。



因为计算机证书服务配置比较复杂，且在本系列的《网管员必读——网络安全》一书有详细介绍，所以在此不再介绍“安全通讯”栏中的“证书”配置。

(4) 单击图 5-24 所示的对话框中“连接控制”栏中的【连接】按钮，打开如图 5-26 所示的对话框。在这里可以设定连接到此 SMTP 虚拟服务器的客户端计算机。如果全部未配置，则默认允许所有人连接使用 SMTP 服务器，通常不需要配置。

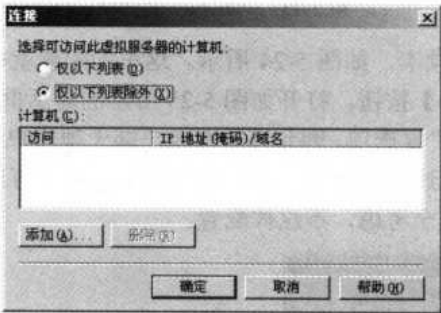


图 5-26 “连接”对话框

如果要排除某些人，或者 SMTP 服务器仅允许部分人使用，则可以在此对话框中配置。可以有两种配置方式：如果选择了“仅以下列表”单选项，则拒绝除列出的特定地址和域之外的所有其他 IP 地址的访问权限。如果选择“仅以下列表除外”复选项，则将访问权限授予除列出的特定地址和域之外的所有 IP 地址。

具体的计算机账户可以通过单击【添加】按钮，打开相应对话框添加。如果要删除原来已添加的计算机账户，则可直接选择该账户，然后单击对话框中的【删除】按钮即可。具体操作非常简单，在此不再赘述。

(5) 单击图 5-24 所示的对话框中“中继限制”下的【中继】按钮，打开如图 5-27 所示的对话框。在这里是用来设置可以使用该 SMTP 虚拟服务器作为 SMTP 中继服务器的客户端计算机账户。设定方法与上一步的“连接”计算机账户设定方法一样，不再赘述。但如果选

择了“允许所有通过身份验证的计算机进行中继，而忽略上表”复选项，则凡是通过了身份验证的计算机账户，都可以使用该服务器的中继服务，不再考虑上面的限制列表。但如果不是通过了身份验证的计算机账户，则仍按上面的限制列表执行。

(6) 在如图 5-24 所示的对话框中单击“邮件”选项卡，如图 5-28 所示。在这里可以设置 SMTP 服务器中客户端发送邮件的大小限制、会话连接限制、每个连接的邮件数限制、每个邮件的收件人数限制、邮件副本、死信目录等进行设置。

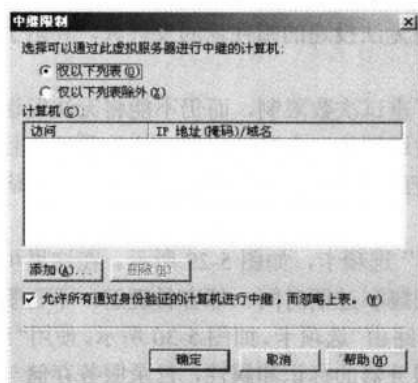


图 5-27 “中继限制”对话框



图 5-28 “默认 SMTP 虚拟服务器属性”对话框“邮件”选项卡

如果选择了“限制邮件大小为 (KB)”复选项，则可设置 SMTP 服务将通知 SMTP 虚拟服务器可接收的最大邮件大小（以千字节为单位）。如果邮件客户端发送的邮件超过了此限制，它将收到一条错误消息。默认值为 2048KB，最小值为 1KB。若要不加限制，请清除此复选项的选择。

如果选择了“限制会话大小为 (KB)”复选项，则可设置整个连接过程中接受的最大数据量（以千字节为单位）。它是连接过程中发送的所有邮件的总和（仅限于邮件正文）。设置此最大值时必须特别谨慎，因为连接邮件传输代理 (MTA) 可能会反复提交邮件，默认大小为 10240KB。此数值应该大于或等于“限制邮件大小为 (KB)”的数值。若要不加限制，请清除此复选项的选择。

如果选择了“限制每个连接的邮件数为”复选项，则可以限制在一次连接中发送的邮件数。默认值为 20 封。利用这种方法，可以通过多个连接向远程域发送邮件，从而提高系统性能。达到所设定的限制之后，系统将自动打开一个新的连接，并继续传输邮件，直到所有邮件传递完毕。要禁用此功能而不设置此限制，请清除此复选项的选择。

如果选择了“限制每个邮件的收件人数为”复选项，则可限制每个邮件的最大收件人数。默认值为 100 个，这是“征求意见稿文件 (RFC) 821”中指定的“最小要求值”。若要禁用此功能而不加限制，请清除此复选项的选择。



某些客户端在收到表明已超过最大收件人数的错误消息后，会返回一封邮件并附有未传递报告（NDR）。在这种情况下，运行 SMTP 的服务器就不会返回带有 NDR 的邮件。它将立即打开一个新连接并处理剩余的收件人。例如，如果收件人数限制为 100，且正在传输一封具有 105 个收件人的邮件，则在收到错误消息之后，将在一个连接中传递发往前 100 个收件人的邮件。然后，系统会打开一个新连接并将邮件发送给剩余的 5 个收件人。

在“将未传递报告的副本发送到”文本框中，可以设置在有无法传递的邮件时的 NDR 副本发送到一个特定的 SMTP 信箱。同时系统会将无法投递的邮件返回发件人，并附上一个未传递报告（NDR）。

在“死信目录”文本框中，可以设置在到达了重试次数限制，而仍不能将无法发送邮件的 NDR 发送给发件人时，将此邮件的一个副本发送到的一个目录位置，这就是死信目录。死信目录中的邮件不能被传递或返回。请定期检查此目录并处理这些邮件，因为一个满的目录会对 SMTP 服务性能带来负面影响。

(7) 在如图 5-24 所示的对话框中单击“传递”选项卡，如图 5-29 所示。在这里可以设置对于不能一次发送成功的邮件重试发送的时间间隔和过期时间。都容易理解，不再赘述。

(8) 在如图 5-29 所示的对话框中单击“LDAP 路由”选项卡，如图 5-30 所示。使用“LDAP 路由”选项卡指定用于 SMTP 虚拟服务器的目录服务器的标识和属性，目录服务存储与邮件客户端及其邮箱有关的信息。SMTP 虚拟服务器使用“轻便目录存取协议（LDAP）”与目录服务进行通信。

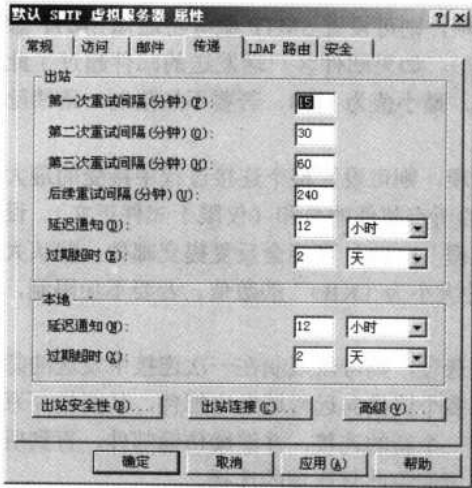


图 5-29 “默认 SMTP 虚拟服务器属性”对话框“传递”选项卡

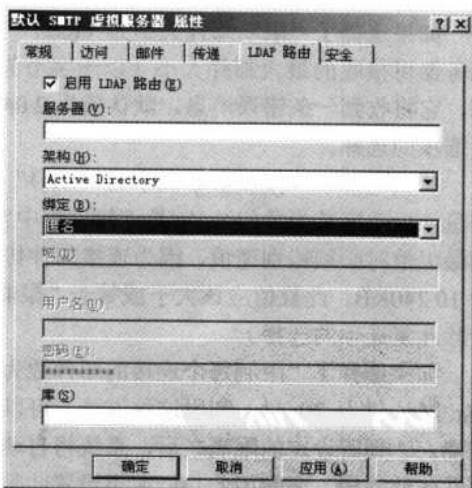


图 5-30 “默认 SMTP 虚拟服务器属性”对话框“LDAP 路由”选项卡

可以配置 SMTP 服务通过 LDAP 服务器解析发件人和收件人。例如：可以使用 Active Directory 作为 LDAP 服务器，并使用“Active Directory 用户和计算机”创建一个可在 SMTP 虚拟服务器上自动扩展的组邮件列表。因为在实际企业邮件服务器应用不多，所以在此不作介绍。系统默认不启用 LDAP 路由服务。

(9) 在如图 5-29 所示的对话框中单击“安全”选项卡，如图 5-31 所示。使用“安全”选项卡将 Windows 用户账户和组添加到 SMTP 虚拟服务器操作员列表中，操作员有权限访问并配置 SMTP 服务器。系统默认是系统管理员组（Administrators）、安装终端服务后创建的“Local Service”（本地服务）和“Network Service”（网络服务）这 3 个组的成员。如果没有终端服务器，可删除“Local Service”和“Network Service”这两个组。当然也可以把其他用户和组成员添加到列表中，使他们成为 SMTP 服务器的操作员。

添加的方法是通过单击【添加】按钮，在打开的对话框选择对应的用户账户即可。如果认为原来添加的用户不再需要具备 SMTP 操作权限，则可以选择对应账户，然后单击【删除】按钮删除。

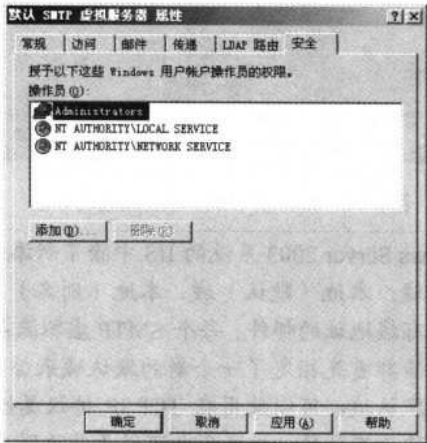


图 5-31 “默认 SMTP 虚拟服务器属性”对话框“安全”选项卡

2. 邮件域的 SMTP 服务属性配置

除了可以统一对 SMTP 服务器进行属性配置外，还可以对具体的邮件 SMTP 服务属性进行配置，方法和所需配置的选项都很简单。只需在“默认 SMTP 虚拟服务器”项下的“域”选项中选择对应的邮件域名选项（本例为 mail.grfwgz.com），单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，即可打开如图 5-32 所示的属性对话框。

在这里仅需要设置 SMTP 服务器的“投递目录”。它是所有传入本地邮件都将被传递到为默认域设置的投递目录中，没有具体的用户信箱。创建的所有别名域都使用同一个投递目录。如果某个目录是 SMTP 服务所在驱动器的本地目录，并且未被指定为拾取目录，则可将其指定为投递目录。在默认情况下，它是邮件根目录的子目录。若要选择其他位置，请单击【浏览】按钮重新选择。

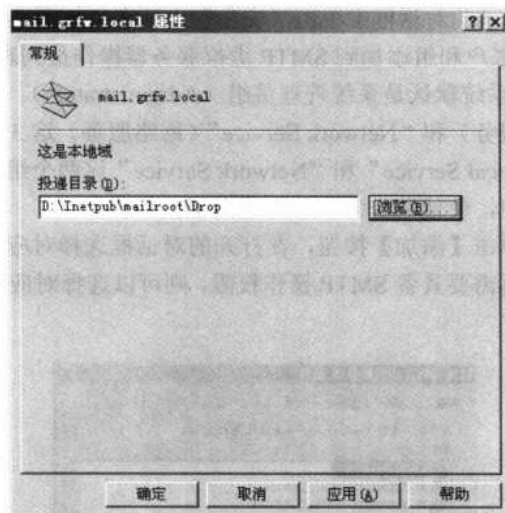


图 5-32 邮件域 SMTP 服务属性对话框



在 Windows Server 2003 系统的 IIS 中除了新添加的邮件域外，系统默认还有另外的邮件域：本地（默认）域、本地（别名）域。“本地（默认）域”用于标记发自没有域地址的邮件。每个 SMTP 虚拟服务器都有一个默认域。不能删除默认域，除非首先指定了一个新的默认域来替代它。

若要命名默认域，可以使用在 TCP/IP 协议属性对话框中“DNS”选项卡上指定的名称作为默认域。此域名也可用于其他服务。或者可以指定一个唯一的域作为 SMTP 服务的专用默认域。启动时，在“DNS”选项卡上指定的域名称将自动用于默认域。如果更改了“DNS”选项卡上的名称，新名称将在下次启动服务时自动用于默认域。无须执行任何操作来更新 SMTP 服务的默认域。

“本地（别名）域”可以设置一个本地别名域，使其设置与默认域相同。SMTP 服务接收的本地别名域邮件将以默认域名进行标记，并放置在为默认域指定的投递目录中。

5.4 POP3 邮件系统的高级配置

在 Windows 2000 Server/Server 2003 系统中的 POP3 服务邮件系统中，没有提供专门的用户邮箱配置功能，但用户邮箱大小可以通过用户磁盘配额来实现限制。当然相应的 POP3 邮件服务器用户中的邮件存储区所在磁盘分区必须是 NTFS 格式文件系统，FAT、FAT32 格式无法配置磁盘配额。

可以使用磁盘配额来控制 and 限制邮件服务器上个人邮箱所使用的磁盘空间，这样可以确保单个邮箱（通常也能确保邮件存储区）不会占用过多的或无法预计的磁盘空间。否则，将对运行 POP3 服务的服务器性能产生不利影响。例如，如果邮件服务器突然收到大量未经请求的电子邮件，邮件存储区会迅速扩大，并有可能占用硬盘上所有可用的磁盘空间。而使用

磁盘配额，邮件存储区将只扩大到指定的配额限制。此时，服务器不再接收邮件，而服务器的其他部分工作正常。但对于不同的邮件系统身份验证方式，磁盘配额的具体作用影响不一样，下面分别予以介绍。

另外，用户发送邮件也必须有一种身份验证方式，以确保邮件服务器的安全。本节将具体介绍各种特发邮件的身份验证方法。

5.4.1 非安全密码身份验证方式下的磁盘配额配置

如果使用 Active Directory 集成的身份验证或本地 Windows 账户身份验证，那么，在默认情况下，发送到 POP3 服务邮箱的电子邮件将文件所有权指派给邮箱用户。在邮箱目录中创建一个配额文件，该文件包含与该邮箱对应的用户账户的安全标识符（SID）。这样文件所有权就会指派给与该配置文件中的 SID 相关的用户账户。NTFS 文件系统的磁盘配额系统也使用 SID 来增强指派给与该 SID 匹配的用户账户的配额限制。发送到该邮箱的邮件存储目录的所有电子邮件，都将被包含在配额文件中的 SID 进行标记。这样，配额系统就可以监控被标记的电子邮件。磁盘配额的配置方法如下。

（1）在资源管理器的邮件存储区所在分区上（必须为 NTFS 格式）单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，然后在打开对话框中选择“配额”选项卡，如图 5-33 所示。

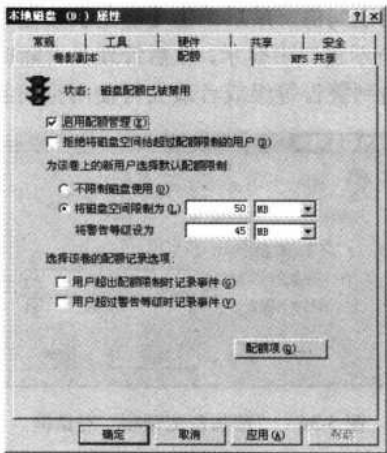


图 5-33 NTFS 格式磁盘分区属性对话框“配额”选项卡

（2）选择“启用配额管理”复选项，然后选择“将磁盘空间限制为”单选项，在其后的文本框中设置一下新用户默认的最大使用空间（本示例为 50MB），然后在下面的“将警告等级设为”文本框中设置一下比最大使用空间小一些的空间（本示例为 45MB），这样当用户使用的空间达到这个值时，系统会发出警告，提醒用户和管理员。如果选择了“拒绝将磁盘空间给超过配额限制的用户”复选项，则用户所使用的磁盘空间达到了最大限制时，将拒绝相应用户在该分区上存储新文件了，除非删除原来已存储的文件，并且新文件存储后的总使用空间在最大空间限制范围之内。

278 网管员必读——网络应用（第2版）

如果同时选择了“用户超出配额限制时记录事件”复选项，则当相应用户所使用的空间超出配额的最大空间限制时就记录事件在事件日志中；如果同时选择了“用户超过警告等级时记录事件”复选项，则当相应用户所使用的空间大小超过上面所设置的警告等级时，也在事件日志中记录该事件，通常不选择。

以上所设置的是针对以后创建的新用户的通用配置，如果想对已存在用户设置配额，则可单击对话框中的【配额项】按钮，打开如图 5-34 所示的窗口。

(3) 要添加新的配置，可执行【配额】→【新建配额】菜单操作，打开如图 5-35 所示的对话框。在这里首先要选择创建新配置的用户对象。

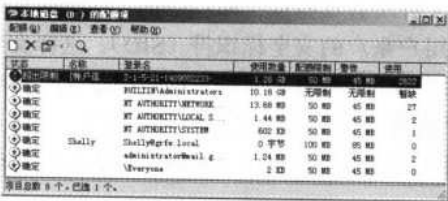


图 5-34 磁盘的配额项窗口

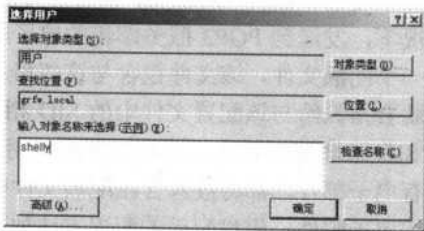


图 5-35 “选择用户”对话框

(4) 单击【确定】按钮，打开如图 5-36 所示的对话框。在这里就可以设置已存在用户的磁盘配额限制了。当然，首先是选择“将磁盘空间限制为”单选项，然后依次设置最大可使用空间值和警告等级可使用空间值。最后单击【确定】按钮即可完成对应已存在用户的磁盘配额配置。并在如图 5-34 所示窗口中显示，以后管理员可随时在这里查看每个用户的磁盘配额使用情况，及时对即将达到警告等级或者最大可使用空间的用户提出警告。

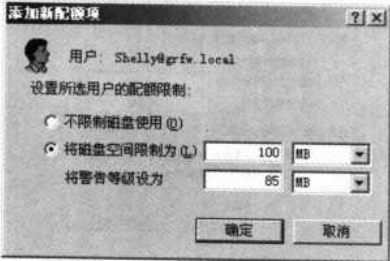


图 5-36 “添加新配额项”对话框

以上就是磁盘配置的基本过程，在非安全密码身份验证方式下，以上配置就会直接影响 POP3 邮件服务器系统中用户邮箱的大小限制（但磁盘配额最大空间值不一定是用户邮箱大小值，因为存储在同一磁盘分区中，但不是邮件存储区中的文件同样属于磁盘配额所计算的范畴）。至于磁盘配额的管理方面，将在《网管员必读——Windows Server 2003 网络管理》一书中具体介绍，在此不再赘述。

5.4.2 使用安全密码身份验证方式下的磁盘配额应用

如果 POP3 邮件系统使用的是加密密码文件身份验证方式，则以上配额系统对于邮箱的

用户账户就会失效。然而，可以使用 `createquotafile` 命令，手动将指定邮箱与一个有效的、已配置了磁盘配额的用户账户关联起来。该关联仅用于磁盘配额目的，与邮箱的身份验证无关。如果是使用 Active Directory 集成的身份验证或本地 Windows 账户身份验证，创建邮箱时将默认创建配额文件。

配额文件的创建步骤很简单，只需进入命令提示符状态，键入：`winpop createquotafile username@domain [/user: username]`命令，其中的“`winpop createquotafile`”命令是用于创建配额文件的；`username@domain` 参数用来指定创建配额文件的用户；`/user: username` 参数用于关联现有用户账户的配额文件创建配额文件。要查看该命令的完整语法，请在命令提示符下键入：`winpop help` 命令。



注意

如果超出了邮箱配额，用户不会收到通知。发给该用户的电子邮件不会被接收，并且将返回一封未送达报告（NDR），通知发件人该电子邮件没有发送到收件人。所以建议管理员在确保用户将电子邮件客户端配置成当成功检索到电子邮件后，就将其从服务器中删除。如果用户将已经成功检索的电子邮件留在服务器上，很快就会超出配额。用户很容易忽视磁盘使用情况和存储在服务器上的旧电子邮件的影响。

另外，无法为 Administrators 组的成员，或 Administrators 账户设置配额限制。

5.4.3 邮件发送配置

在邮件服务器系统中，邮件发送配置往往要比邮件接收配置复杂，因为它不仅涉及到身份验证，还涉及到发送连接数限制、发送目标域等方面。下面分别予以介绍。

1. 邮件发送身份验证方法的配置

可以配置简单邮件传输协议（SMTP）虚拟服务器，以提供接收服务器所要求的身份验证凭据。有 3 类可用的身份验证：匿名、基本（明文）和集成 Windows 身份验证。匿名不需要进行身份验证。选择明文选项，你所连接的服务器的账户名称和密码会以明文方式进行传输。集成 Windows 身份验证选项要求提供 Windows 账户名称和密码。

为特定的远程域可重写此处的选项集。为远程域重写身份验证设置的功能可以设置虚拟服务器的身份验证级别，以处理大多数的传输，同时允许单个地址有例外情况。表 5-4 描述了几个配置示例。

表 5-4 SMTP 服务器身份验证方式选择示例

SMTP 传输	身份验证选项
通常将邮件发送到多个地址	禁用 SMTP 虚拟服务器的验证。如果到某个地址的邮件传递操作由于身份验证要求而失败，则为该地址添加一个远程域。然后，在服务器要求的相同级别上启用该域的身份验证
通常将邮件发送到某个地址（要求进行身份验证）	确定连接所需的身份验证级别。然后，使用相同的级别启用 SMTP 虚拟服务器的身份验证。如果随后要将邮件发送到其他地址，则建立远程域并设置不同的身份验证选项。如果使用此选项，则使用的账户名可能就是用于标识设置为中继主机的计算机的账户名

身份验证的配置步骤如下。

- (1) 在 IIS 管理器中，在 SMTP 虚拟服务器上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“传递”选项卡，参见图 5-29。
- (2) 单击【出站安全性】按钮，打开如图 5-37 所示的对话框。如果选择“匿名访问”单选项，并清除其他复选项的选择，则用户在向外发送邮件时就不需要进行身份验证了。

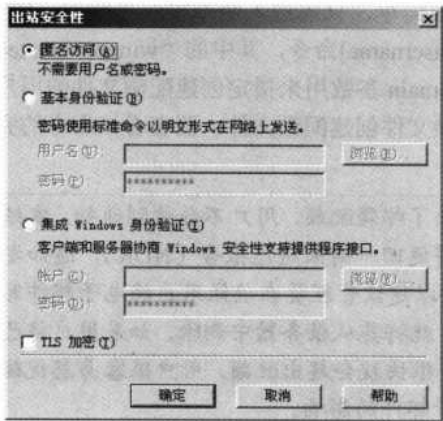


图 5-37 “出站安全性”对话框

如果选择的是“基本身份验证”单选项，将以明文形式传输正在连接的服务器的账户名和密码。此选项要求配置用户名和密码，也可通过单击【浏览】按钮，在打开的对话框中选择用户。此设置应与接收服务器的传入（POP3）身份验证要求相匹配。

如果选择的是“集成 Windows 身份验证”单选项，此选项要求提供 Windows 用户账户名和密码。此项身份验证方式也需要配置用于身份验证的用户名和密码，同样也可通过单击【浏览】按钮，在打开的对话框中选择用户，此设置也应与接收服务器的传入身份验证要求相匹配。如果要使用 SMTP 服务器的中继服务，就必须选择“集成 Windows 身份验证”的验证方式。

如果在选择以上身份验证方式的同时选择了“TLS 加密”复选项，则要求所有传出邮件都使用“传输层安全（TLS）”进行加密。

- (3) 选择并配置好身份验证方式后，单击【确定】按钮即可完成配置。



注意 从以上的身份验证方式配置可以看出，这种 POP3 邮件系统仅用于局域网内部，因为所有人的身份验证都使用了相同的用户账户。

2. 出站连接配置

出站连接配置是在如图 5-29 所示“传递”选项卡中单击【出站连接】按钮，打开如图 5-38 所示的对话框进行配置。

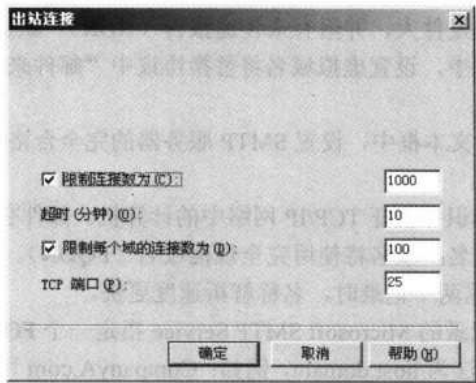


图 5-38 “出站连接”对话框

对于出站连接，在“限制连接数为”文本框中，定义可同时连接到远程域的出站连接总数。此复选框默认被选中，默认限制是 1 000。最小连接数为 1。对于传入和传出连接，必须选中此复选项，相应限制才能生效。

在“超时（分钟）”文本框中，在指定时间内，如果某一连接始终处于非活动状态，则 Microsoft SMTP Service 将关闭此连接。可以指定此时间段。对于传入和传出连接，默认时间都是 10 分钟。

在“限制每个域的连接数为”文本框中，限制可以连接到单个远程域的传出连接数。默认值为 100。此数值应小于或等于为“限制连接数为”设置的值。

在“TCP 端口”文本框中指定用于传出传输的 TCP 端口。默认端口是 SMTP 标准 TCP 端口 25，不要更改。

3. 邮件发送的高级配置

邮件发送的高级配置是在如图 5-29 所示“传递”选项卡中单击【高级】按钮，打开如图 5-39 所示的对话框进行配置。

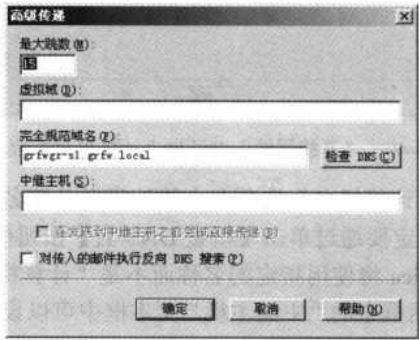


图 5-39 “高级传递”对话框

在“最大跳数”文本框中，可设置传递邮件时，邮件在到达最终目的地前可能要经过多个服务器。可以指定允许邮件通过的服务器数目。通常称为“跳数”。设置跳数之后，SMTP 服务器将对邮件头的“已收到”行中的跳数进行计数。当“已收到”字段的数值超过最大跳

282 网管员必读——网络应用（第2版）

数设置时，邮件将被退回发件人，并附有未传递报告（NDR）。默认跳数值为 15。

在“虚拟域”文本框中，设置虚拟域名将替换协议中“邮件来自于”行中的本地域名。可不配置。

在“完全规范域名”文本框中，设置 SMTP 服务器的完全合格域名。通常系统默认显示了，不用另外配置。

可以使用两个记录标识并验证 TCP/IP 网络中的计算机。邮件交换程序（MX）记录标识主机及与计算机相关的域名。域名将使用完全规范域名（FQDN）。地址（A）记录标识计算机的 IP 地址。同时使用这两个记录时，名称解析速度更快。

必须为要处理 MX 记录的 Microsoft SMTP Service 指定一个 FQDN。FQDN 被 DNS 用来标识域的主机服务器。语法为 host.domain，例如：CompanyA.com 可能具有数个主机服务器，其中之一名为 Server01。则此服务器的 FQDN 将为 Server01.CompanyA.com。

可以通过以下两种方法指定 FQDN。可以使用“控制面板”中“系统特性”的“计算机名”选项卡（如图 5-40 所示）上指定的名称，或者为正在配置的 SMTP 虚拟服务器指定唯一的 FQDN。启动时，在“系统特性”的“计算机名”选项卡上指定的名称将自动用于 FQDN。如果手动或通过加入域更改名称，新名称将在下次启动计算机时自动用于 FQDN，而无须执行任何操作来更新 SMTP 虚拟服务器的 FQDN。

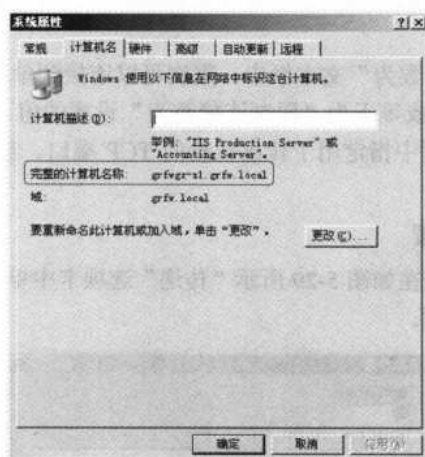


图 5-40 “系统属性”对话框“计算机名”选项卡

若要覆盖自动使用的“计算机名”选项卡上的计算机及域名，请在这里的“高级传递”选项卡上更改 FQDN，但一定要通过单击【检查 DNS 名】按钮检查所设置的名称是否有效。然后，Microsoft SMTP Service 将使用指定的名称而不是“计算机名”选项卡上指定的名称。

在如图 5-39 所示的对话框中的“中继主机”文本框中可以设置邮件传递的中继主机，这样就可以通过中继主机将所有传出邮件路由到远程域，而不是直接发送。这种邮件路由连接方式比其他路由方式更直接、成本更低。中继主机类似于远程域的路由域选项。区别在于指定中继主机之后，所有传出邮件都将路由到此服务器。而使用路由域时，只有远程域的邮件被路由到特定服务器。

即使设置了中继主机，仍可以为远程域指定一个不同的路由。路由域设置将覆盖中继主

机设置。在此键入 FQDN 或 IP 地址以标识中继主机。如果使用 IP 地址，请将它用 “【】” 括起来以提高系统性能。Microsoft SMTP Service 首先检查名称，然后检查 IP 地址。括号将该值标识为 IP 地址，从而绕过 DNS 搜索。

配置了中继主机以后，“在发送到中继主机之前尝试直接发送”复选项才会生效。选中此复选项时，Microsoft SMTP Service 会在将远程邮件转发到中继主机服务器前尝试直接发送。默认设置是将所有远程邮件发送到中继主机，而不是直接发送。

如果选择了“对传入的邮件执行反向 DNS 搜索”复选项，则 Microsoft SMTP Service 将试图验证客户端 IP 地址是否与 EHLO/HELO 命令中客户端提交的主机/域相匹配。如果反向 DNS 搜索成功，“已收到”头将完整保留；如果验证失败，邮件的“已收到”头中的 IP 地址后面将显示“未验证”；如果 DNS 搜索失败，邮件的“已收到”头中将显示“RDNS 失败”。

但需要注意的是，由于此功能将验证所有传入邮件的地址，所以使用它会影响 Microsoft SMTP Service 的性能。

5.5 客户系统的配置

POP3 邮件系统的客户系统配置主要包括在 POP3 服务器中创建用户邮箱账户，然后在客户端邮件程序中配置用户账户。

5.5.1 客户端邮箱的创建

POP3 和 SMTP 服务器属性都配置好后，接下来就要在 POP3 服务控制台中为客户端创建对应的用户邮箱了。操作方法如下。

(1) 在如图 5-13 所示的邮件服务器左边窗口中选择相应的邮件服务器域名，单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【邮箱】命令，或者直接在右边窗口中单击“添加邮箱”链接，打开如图 5-41 所示的对话框。在这里可以添加新用户邮箱。

如果所创建的用户邮箱对应的是系统中不存在的用户，则要选择“为此邮箱创建相关联的用户”复选项，输入好邮箱名和密码后单击【确定】按钮，系统会弹出如图 5-42 所示的提示。在提示中提醒了用户在使用不同身份验证方式下的用户邮箱账户名称。

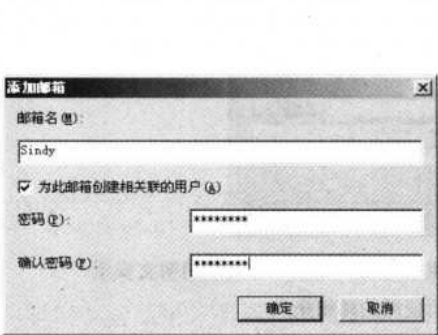


图 5-41 “添加邮箱”对话框

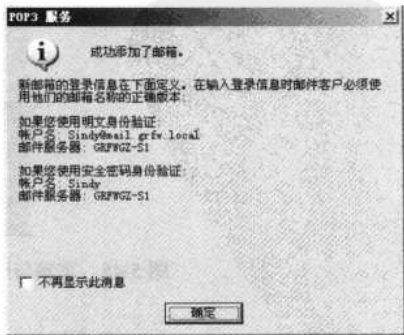


图 5-42 “POP3 服务”提示框



注意

当所创建的用户邮箱名与域系统中已有用户账户名一样时，就不要选择“为此邮箱创建相关联的用户”复选项了，直接输入与用户账户一样的邮箱名即可。这样，系统会自动在他们的用户账户中配置以邮件服务器域名为后缀的电子邮件地址，如图 5-43 所示。否则将创建一个以所输入的用户名+“000”为用户名的用户账户（在 Windows 系统中也将同时创建这样一个用户账户），就像图 5-44 中提示那样的 Shelly000，这是因为原来在系统中已存在一个 Shelly 用户账户，不过此账户也仅在使用安全密码身份验证方式时使用，使用明文身份验证时仍使用原账户名称，如图 5-45 所示。但在 Windows 2000 混合域模式下，如果在域中已存在相同的账户，则一定不能在为用户创建邮箱时，在如图 5-41 所示的对话框中选择“为此邮箱创建相关联的用户”复选项，否则拒绝创建。



图 5-43 用户属性对话框“常规”选项卡

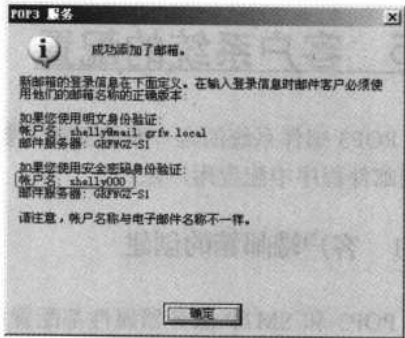


图 5-44 重建与原系统中用户重名的用户邮箱时的系统提示



图 5-45 重建与原系统中用户重名的用户邮箱，并且采用明文安全验证方式时所使用的邮箱账户

(2) 添加了用户邮箱后的邮件服务器窗口如图 5-46 所示。此时在“状态”列中显示“已

解锁”，表示用户可以使用邮箱了。如果要禁用某用户的邮箱，则只需在相应用户邮箱上单击鼠标右键，在弹出的快捷菜单中选择【锁定】命令即可。

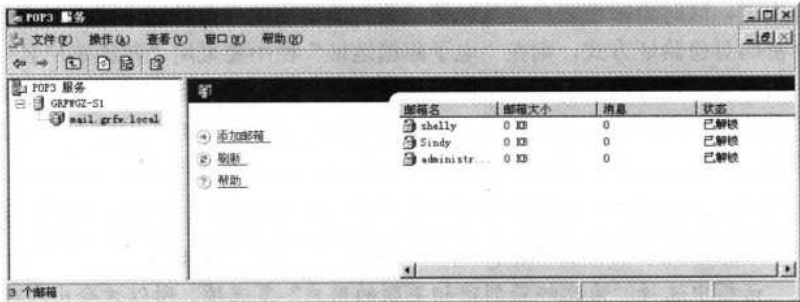


图 5-46 添加了用户邮箱的邮件服务器窗口



除了可以向已有域邮件服务器中添加用户邮箱外，还可以在邮件服务器添加多个隶属于不同域，或者工作组系统的邮箱系统，为不同域，或工作组提供邮件服务。方法是在如图 5-13 所示的 POP3 邮件服务器窗口中选择邮件服务器，然后在右边的窗口中单击“新域”链接，打开的对话框参见 5-18。在其中输入新的邮件服务器域名，单击【确定】按钮即可。这样，在一个邮件服务器中就可以为多个不同域系统担当邮件服务器角色。

5.5.2 POP3 系统邮件客户端配置

最后以大家常用的 Outlook Express (OE) 为例介绍企业内部邮件系统中的客户端软件配置，Outlook 的配置方法与 Outlook Express 的配置方法基本一样，参照即可。
客户端的配置很简单，但有一个要注意的地方就是不同的身份验证方式对应在的邮箱用户账户也不一样，这一点已在 5.5.1 节中说明了。本示例以 Windows 集成的明文身份验证方式的企业内部邮件系统配置为例进行介绍。

(1) 在 OE 中执行【工具】→【账户】菜单操作，在打开的对话框中选择“邮件”选项卡，如图 5-47 所示。



图 5-47 “Internet 账户”对话框“邮件”选项卡

(2) 单击【添加】按钮下的“邮件”，打开如图 5-48 所示的对话框。在这里的配置方法

与其他邮箱账户的配置一样，需配置一个用于识别和接收邮件方显示的账户名称。

(3) 单击【下一步】按钮，打开如图 5-49 所示的对话框。在这里要为用户配置相应的邮箱账户。不过，这时原邮箱账户的具体格式要视所采用的身份验证方式来确定。如果采用的是非安全密码身份验证方式，则在“电子邮件地址”栏中要采用“邮箱账户名+@+邮件服务器域名”的格式。与我们平常的电子邮箱地址结构一样，参见图 5-49。通常是这种配置。但是如果采取的安全密码身份验证方式，则这里的“电子邮件地址”中就不能加上邮件服务器域名后缀了，直接把系统中的用户账户名给出即可，如图 5-50 所示。

注意 邮箱账户名与邮箱名可能不一样，参见图 5-44 所示的 Shelly 用户项。由于原系统中已存在 Shelly 用户，而在创建用户邮箱时又在如图 5-41 所示的对话框中选择“为此邮箱创建相关联的用户”复选项，所以才会出现邮箱用户账户名（Shelly000）与邮箱名（Shelly）不一样的现象。但在图 5-49 和图 5-50 所示的对话框中的“电子邮件地址”中输入的是邮箱账户名，而不是邮箱名。

(4) 无论采用哪种身份验证方式，在如图 5-49 或者图 5-50 所示的对话框中单击【下一步】按钮，打开如图 5-51 所示的对话框。在“接收邮件（POP3）”和“发送邮件服务器（SMTP）”两个服务器地址，千万不要把它设置成邮件域名，而是要设置为邮件服务器的计算机名（也可以是对应的 IP 地址）。

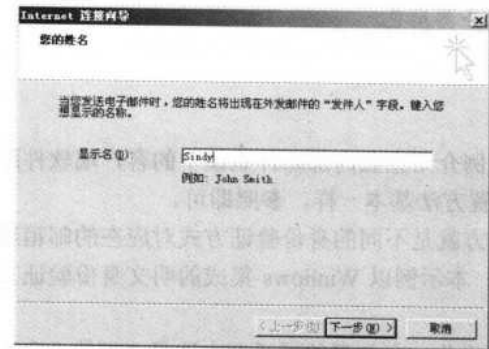


图 5-48 “你的姓名”对话框

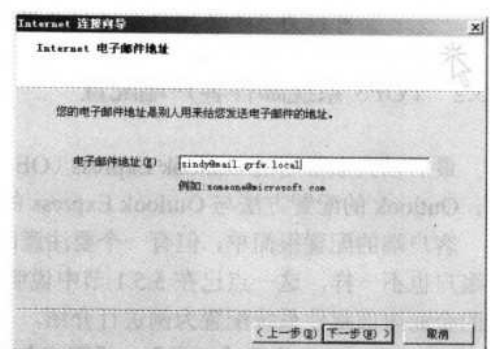


图 5-49 采用非安全密码验证方式时的邮箱配置格式

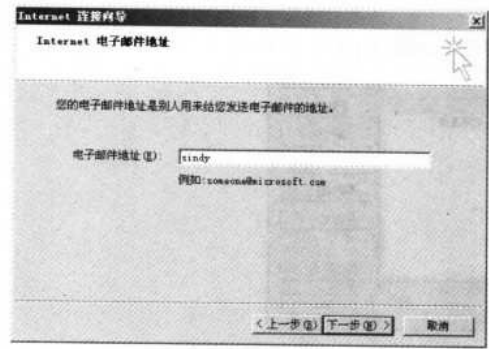


图 5-50 采用安全密码验证方式时的邮箱配置格式

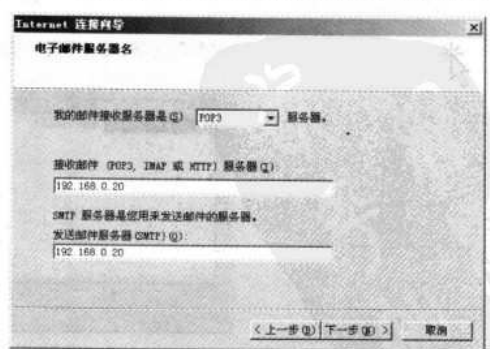


图 5-51 “电子邮件服务器名”对话框

(5) 单击【下一步】按钮，打开如图 5-52 所示的对话框。此处的电子邮件账户名配置

方法一样，对应不同的身份验证方式。当采用集成式非安全密码的 Windows 身份验证时，电子邮件账户名称后面一定要加上邮件服务器域名后缀，参见图 5-52，此时不要选择“使用安全密码验证登录”复选项；如果是采取安全密码身份验证方式，则无须后面的域名后缀，参见图 5-53，不过，此时一定要选择“使用安全密码验证登录”复选项。

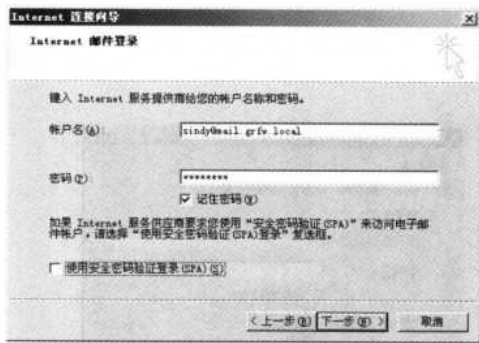


图 5-52 采用非安全密码验证时的“账户名”配置

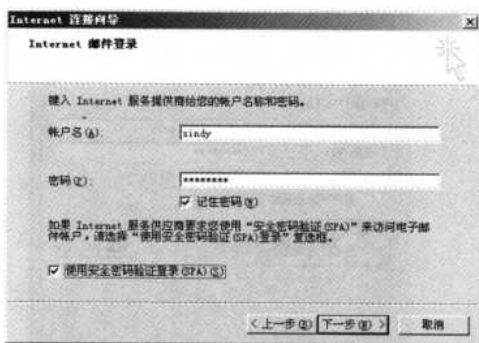


图 5-53 采用安全密码验证时的“账户名”配置

(6) 无论采用哪种身份验证方式，在如图 5-52 或者图 5-53 所示的对话框中，单击【下一步】按钮，打开一个向导完成对话框，如图 5-54 所示。单击【完成】按钮完成新账户的创建与配置。

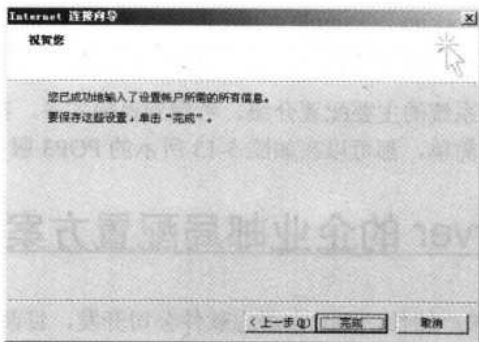


图 5-54 邮箱创建向导完成对话框

以上是新建邮箱账户时的配置方法，如果要修改现有邮箱账户，以应用于当前 POP3 邮件系统，则只需在相应对话框中的对应选项按以上方法配置即可，主要是需要区别不同的身份验证方式。不过通常是采用非安全密码（也就是不采用 SSL 连接），所以在账户名后面一定要加上 POP3 邮件服务器域后缀。

对于发送邮件，如果在如图 5-37 所示的对话框中选择了“基本身份验证”或者“集成 Windows 身份验证”两种方式，并且配置了身份验证账户，则相应用户的 SMTP 身份验证配置也需要相同的账户信息。配置方法是在如图 5-55 所示的对话框中选择“我的服务器要求身份验证”复选项（如果在如图 5-37 所示的对话框中选择的是“匿名访问”单选项，则不要选择此复选项），然后单击【设置】按钮，打开如图 5-56 所示的对话框。在其中选择“登录方式”单选项，然后在下面的“账户名”和“密码”文本框中输入在如图 5-37 所示的对话框中

288 网管员必读——网络应用（第2版）

配置的用于身份验证的用户名和密码信息。如果要采用 SSL 安全连接，则要选择“使用安全密码验证登录”复选项。

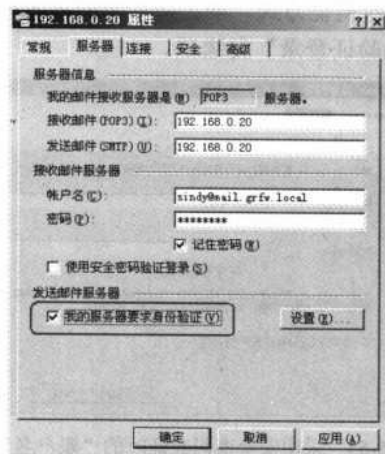


图 5-55 用户邮箱账户属性对话框“服务器”选项卡

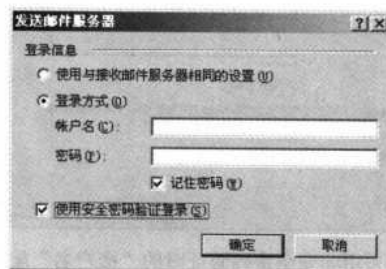


图 5-56 “发送邮件服务器”对话框



以上 SMTP 服务器的身份验证配置同样适用于 SMTP 中继，此时在“账户名”文本框中键入不包括对方邮件域域名的 POP3 用户邮件账户名。例如，如果邮箱为 someone@example.com，需键入：someone；在“密码”文本框中键入对方邮件域相应 POP3 邮件账户的密码。

以上就是 POP3 邮件系统的主要配置介绍，考虑到篇幅关系，在此就不介绍 POP3 邮件系统的管理了，其实也很简单，都可以在如图 5-13 所示的 POP3 服务器控制台窗口中进行。

5.6 CMailServer 的企业邮局配置方案

CMailServer 是一款国产软件，由北京遥志软件公司开发，目前的最新版本为 5.4.1。它也是应用最广、配置最为容易、性能最稳定的一款企业邮件服务器软件。其试用版可以在 <http://www.youngzsoft.com/cn/> 网站上下载。更为难得的是它为全中文系统（包括帮助文件），这对于中、小型企业系统管理员来说具有相当大的帮助。

5.6.1 CMailServer 5.4.1 简介

邮件服务器 CMailServer 于 2000 年 8 月问世，是基于 Windows 平台的邮件服务器软件，支持互联网邮件收发、网页邮件收发（Webmail）、邮件杀毒、防垃圾邮件、邮件过滤、邮件监视、邮件备份、邮件转发、多域名邮件收发和邮件发送验证等功能，是目前国内非常流行的邮件服务器软件和下载量最大的邮件服务器软件。CMailServer 以其设置简单，容易使用，出色的稳定性和灵活的 Web 邮件服务在众多邮件服务器软件中成为一枝独秀。

1. 基本特性

- 支持 Windows 2000、Windows XP、Windows Server 2003 等操作系统。
- 支持通用邮件客户端软件 Outlook Express、Foxmail 等收发邮件。
- 支持 Web 界面收发邮件，有完善的 WebMail 功能。
- 支持 Internet 收发邮件，可以安全快捷往互联网发送邮件。
- 支持用户通过 Web 浏览器申请邮箱、修改邮箱密码和用户信息等资料。
- 支持管理员新建、删除、禁用用户邮箱和设置用户邮箱大小。
- 支持管理员通过浏览器远程管理账号。
- 支持管理员同时向多个用户发送邮件，方便管理员发送通知。
- 支持生成 HTML、INI、Excel 和 Text 多种格式的用户邮箱信息报表。
- 支持作为 NT 服务运行，方便服务器管理。
- 支持 ESMTP 验证，更安全，可以有效地防止垃圾邮件发送者的入侵。
- 支持多域名，可以将多个域名的邮件通过一台邮件服务器统一收发。
- 支持邮件备份，可以保存所有通过邮件服务器发送的邮件。
- 支持完善的日志记录，可以分析邮件服务器用户访问记录。
- 支持邮件组，发往邮件组邮件地址的邮件会自动分发给每个组成员。
- 支持邮件代理，可以接收其他互联网账号邮件。
- 支持邮件杀毒，可以和瑞星、诺顿等杀毒软件结合使用，轻松杀毒。
- 支持邮件过滤和 IP 过滤，操作简单易用。

2. 安装环境建议

服务器的配置跟用户数有关。如果用户数在 20 人以内，推荐使用：CPU PIII 700MHz 以上，内存 128MB，硬盘 10GB；操作系统：Windows 2000 以上，打好系统补丁。

如果用户数在 100~500 人之间，需要选用专业的服务器作为邮件服务器，服务器一定要专用，即专门作为邮件服务器来用。推荐使用：P4 1.7GHz 以上，内存 512MB，硬盘 40GB；操作系统：Windows 2000 Advanced Server 以上，打好系统最新补丁。

如果用户数在 1 000 人以上：推荐使用企业级服务器，服务器一定要专用，即专门作为邮件服务器来用。推荐使用：双 P4 CPU，内存 1GB，硬盘 60GB；操作系统：Windows 2000 Advanced Server 以上，打好系统最新补丁。

安装好操作系统，并安装好 IIS 组件。如果安装了防火墙，请打开 25 端口和 110 端口。CMailServer 要用到这两个端口进行邮件传输。而且建议安装在 NTFS 格式分区中，这样才能为各种邮箱配置用户访问权限，更加安全。

尽管可以使用 Windows 2000 系统，但笔者建议采用的 Windows Server 2003 R2 版本，因为这一版本中的各方面性能和安全性均较 Windows 2000 系统高。

5.6.2 CMailServer 邮件服务器系统的基本配置思路

CMailServer 可配置多种不同功能的邮件服务器，如局域网内部邮件服务器、互联网邮件服务器、局域网拨号邮件服务器、多域名邮件服务器。但它们的设置方法都很简单，所以在此不再对每种邮件服务器的配置进行细分，而是分节介绍各种邮件服务器的主要设置方法。

290 网管员必读——网络应用（第2版）

当然，在这之前还是成功安装并启用相关的服务。下面是以上各种 CMailServer 邮件服务器的共同基本配置思路。

1) 安装 CMailServer 程序，并启用相关服务

程序的安装没什么特别，直接下载试用版，或者购买正式版，然后按照一般 Windows 程序的安装方法安装即可。只是在安装后可能会出现一些问题，如服务端口冲突、邮件服务器无法正常启动等。此时就需检查系统中的相关配置了，在排除了故障后才能正常使用 CMailServer 配置邮件服务器了。

如果在安装后出现如图 5-57 所示的 SMTP 或者如图 5-58 所示的 POP3 服务启动失败。这是因为你的服务器上安装了其他跟邮件服务有关的程序（如 IIS 中的 SMTP 虚拟服务器和 POP3 邮件服务器），造成冲突。CMailServer 会自动检查哪些程序占用了这些端口，并在用户的确认下关闭这些程序。

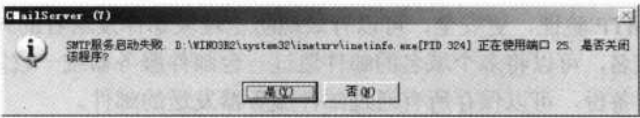


图 5-57 发生 SMTP 端口冲突时的错误提示

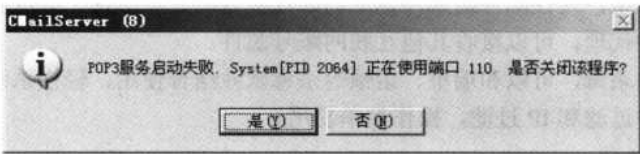


图 5-58 发生 POP3 端口冲突时的错误提示

如果设置虚拟目录失败。这是因为你的机器没有安装好微软的 IIS 服务。如果没有安装 IIS 组件，结束前会提示相应信息，这时其他功能一切正常，只是不能使用 WebMail 功能。因为 CMailServer 会在安装后自动把 WebMail 文件添加到 IIS 的默认网站中，如图 5-59 所示。



图 5-59 自动添加在 IIS 默认网站中的 WebMail 文件

要检查 WebMail 功能是否正常启动，可在本机浏览器的地址栏输入“http://127.0.0.1/mail”即可测试，如果能出现如图 5-60 所示的界面即表示成功。



图 5-60 正常启动后的 WebMail 界面

2) 创建各种类型的邮件服务器

这里所说的邮件服务器就包括局域网内部邮件服务器、互联网邮件服务器、局域网拨号邮件服务器、多域名邮件服务器。

本章以局域网邮件服务器的配置为例在 5.7 节进行邮件服务器设置的全面介绍，互联网邮件服务器、局域网拨号邮件服务器、多域名邮件服务器的设置方法绝大多数可以参照进行，将在 5.8 节介绍。CMailServer 邮件服务器的通用创建与设置方法为：基本配置→高级配置→用户邮箱的创建与配置→客户端邮件程序的配置。

3) 邮件服务器的维护与管理功能

邮件服务器的维护与管理是管理员的日常工作，邮件服务器经常出现的问题就是发送、接收邮件，用户密码忘记了，垃圾邮件的过滤等。具体内容参见 5.9 节。

5.7 局域网邮件服务器的建立与配置

在前面已有介绍，CMailServer 邮件服务器程序可以创建局域网内部邮件服务器、互联网邮件服务器、局域网拨号邮件服务器、多域名邮件服务器等多种类型的邮件服务器。这些邮件服务器的建立与配置并不完全一样。本节和后面各节将分别予以介绍。

5.7.1 局域网内部邮件服务器的基本配置

这里所说的“局域网内部邮件服务器”仅应用于局域网内部员工之间的通信。下面是具体配置方法。



以下所进行的基本设置除了邮件服务器类型选择项设置外，其他的设置均适用于其他类型的邮件服务器。在后面介绍的其他邮件服务器建立配置中不再另行介绍。

(1) 在如图 5-61 所示 CMailServer 程序主界面工具栏中单击【设置】按钮，打开如图 5-62 所示的对话框。在这里首先要选择邮件服务器类型。因为这里要建立的是局域网内部邮件服务器，所以在此选择“作为局域网邮件服务器”单选项。



图 5-61 CMailServer 5.4.1 程序主界面

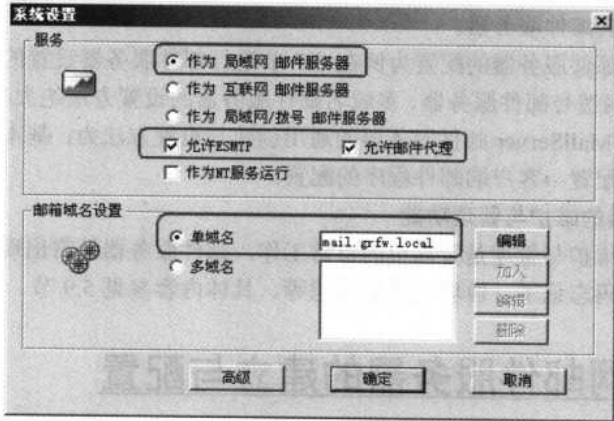


图 5-62 “系统设置”对话框

如果选择了“允许 ESMTP”复选项，则用户发送邮件时必须经过身份认证（也就是不允许匿名通过邮件服务器发送邮件）。这一项是默认选择的，这样可以有效地防止非法用户利用 CMailServer 发送垃圾邮件。但同时要求在客户端的 Outlook 账号设置里也选择“我的服务器要求身份验证”复选项，参见前面的图 5-55。

如果选择了“允许邮件代理”复选项，则 CMailServer 开放其邮件代理功能，这样可以实现客户端通过 CMailServer 代理接收和发送互联网邮件。这一项是默认选择的，可以实现员工互联网邮件的收发，只不过它所对应的域是局域网域，而不是互联网域。

如果选择了“作为 NT 服务运行”复选项，则设置了 CMailServer 作为 NT 服务后台运行，这样可以实现不登录操作系统就可以启动 CMailServer。此功能仅对 Windows NT/2000/XP/Server 2003 系统有效。选择了此复选框后，则该软件将随系统的启动而自动启动。一般不需要这样选择。

如果服务器中只有一个邮件域，则选择“单域名”单选项，将 CMailServer 设置成单一域名的邮件服务器。系统默认的域名是以当前服务器计算机名再加上.com 域名后缀的形式，可直接修改，而且也不要求一定与当前网络域名一样，可以使用更有代表性的个性化域名；

如果服务器中有多个邮件域，则选择“多域名”单选项，将 CMailServer 设置成可以同时支持多个域名的邮件服务器。在此以单域名为例进行介绍。

(2) 单击对话框中的【高级】按钮，即可打开如图 5-63 所示的“高级”对话框。在“互联网邮件”选项卡中通常我们按系统默认设置即可，不需改变原来的配置，而且此选项卡的配置仅适用于要收发互联网邮件的邮件服务器，此处配置的是局域网邮件服务器，则可不作配置。如果企业向 ISP 申请了专门的邮件发送服务器，则可选择“通过 ISP 提供的 SMTP 服务器发送邮件”单选项，然后将相应的 SMTP 服务器地址和所使用的端口配置在下面的“邮件服务器地址”和“端口”文本框中。

(3) 单击“账号”选项卡，如图 5-64 所示。如果选择了“允许通过网页申请账号”复选项，则用户可以直接使用程序所提供的 WebMail 账号申请功能通过网页申请账号。

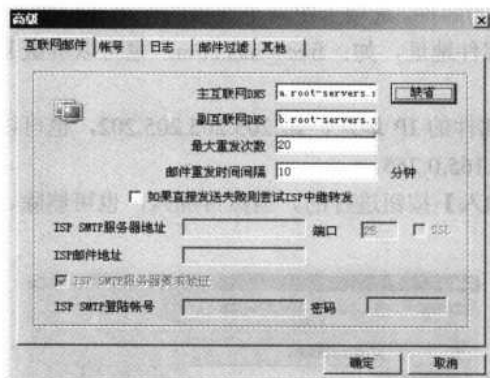


图 5-63 “高级”对话框“互联网邮件”选项卡

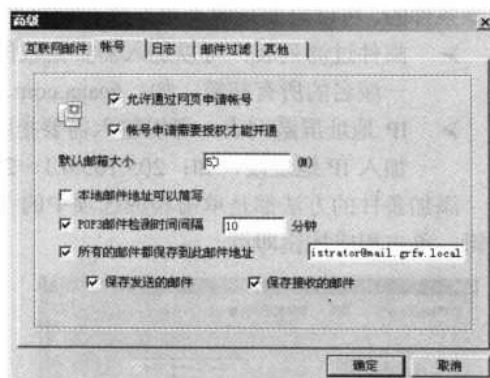


图 5-64 “高级”对话框“账号”选项卡

如果选择了“账号申请需要授权才能开通”复选项，则并不是所有用户都可以成功通过 WebMail 网页来申请账号了，而是需要管理员授权。选择了这项设置后，用户虽然可以申请账号，但是并不能马上开通。需要管理员修改账号设置，才能开通该邮箱账号。从安全角度考虑，建议选取这一复选项。

在“默认邮箱大小”文本框中可设置新用户邮箱的默认大小，系统默认值为 20MB。这个大小将默认作用于所有新用户创建时的邮箱大小设置。

如果选择了“本地邮件地址可以简写”复选项，则向本地用户发送邮件时，可以只填写用户账号，不需要写@邮箱域名。此选项只对单域名有效。

如果选择了“POP3 邮件检测时间间隔”复选项，则可以设置服务器是否自动收取用户设置的 POP3 邮件及收取邮件的时间间隔，默认为每隔 10 分钟检查一次。

如果选择了“所有的邮件都保存到此邮件地址”复选项，则指定将所有通过 CMailServer 发送和接收的邮件保存到此复选项后面的文本框中设定的邮箱中。相当于在服务器上对下面所选定的邮件类型进行备份，这个邮箱账户通常是由管理员管理的。在经过 CMailServer 收发的邮件，在发送到目的邮箱的同时也会发一份到这里所设定的邮箱中。通常出于安全考虑，建议选择这一复选项。选择了这一复选项后，下面的两个复选项才可选，如果选择了“保存发送的邮件”复选项，则上述指定的邮箱中只保存服务器中所有发送出去的邮件；如果选择了“保存接收的邮件”复选项，则上述指定的邮箱中只保存服务器中所有接收到的邮件。系

294 网管员必读——网络应用（第2版）

统默认是两个均选择。

(4) 单击“日志”选项卡，如图 5-65 所示。在这里要设置与邮件日志有关的一些基本选项。CMailServer 日志保存功能能记录服务器的活动情况。

在“保存日志到”文本框中设置 CMailServer 日志文件保存路径。在“最大行数”文本框中设置日志文件中的最大记录行数。

单击下面的对应按钮可以查看相应类型的日志记录。单击【系统日志】按钮，可打开邮件系统运行记录；单击【SMTP 日志】按钮，可打开邮件服务器的邮件发送记录；单击【POP3 日志】按钮，可打开邮件服务器所有接收邮件记录；单击【互联网日志】按钮，可打开邮件服务器所有互联网邮件发送记录；单击【清除日志】按钮，则可清除所有的日志记录。

(5) 单击“邮件过滤”选项卡，如图 5-66 所示。这个选项卡是用来设置邮件和 IP 地址过滤条件的。可以限制接收某用户或计算机发来的邮件。选项卡中两个选项的作用介绍如下。

- 邮件过滤列表：可以加入需要拒收的邮件地址，如：free@aaa.com；也可以屏蔽某一域名的所有邮箱，如：@aaa.com。
- IP 地址屏蔽列表：可以输入需要拒收邮件的 IP 地址，如 205.205.205.202，也可以加入 IP 地址段，如：205.165.0.1~205.165.0.255。

添加条件的方法都是单击相应选项中的【加入】按钮进行的。当然可加入，也可删除、编辑，单击相应按钮即可。

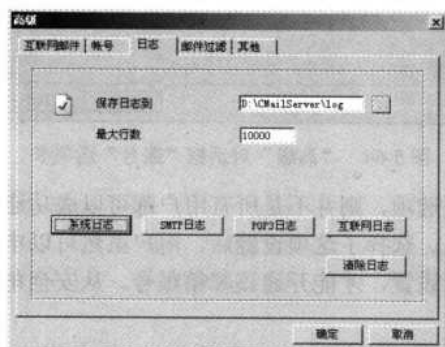


图 5-65 “日志”选项卡

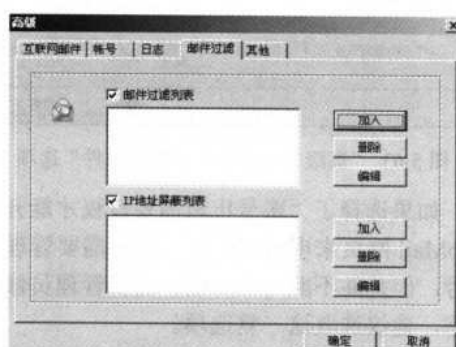


图 5-66 “邮件过滤”选项卡

(6) 单击“其他”选项卡，对话框如图 5-67 所示。在这个选项卡中，我们可以对一些其他杂项进行设置。上面这些选项一般不用重新设置，按系统默认设置即可。下面着重介绍对话框中最下面的 3 个复选项。

如果其他邮件服务器上的用户要借用本邮件服务器来收发互联网邮件，则需选择“代理服务器”复选项，然后单击被激活的【代理设置】按钮，打开类似如图 5-68 所示的对话框，在相应文本框中输入代理服务器 IP 地址或域名和连接所用端口。Socks 服务器一般就是指本 CMailServer 邮件服务器，当然也可以是其他代理服务器，端口号一般不要更改，因为 1080 是 Socks5 协议的专用端口。如果在代理服务器上设置了身份验证，则选择“需要验证”复选项，然后在下面指定用于身份验证的账户，通常也是管理员在代理服务器上的账户。

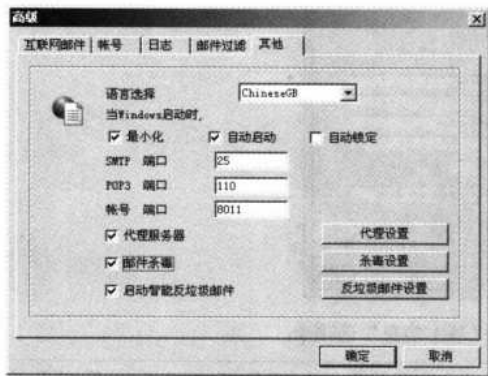


图 5-67 “其他”选项卡

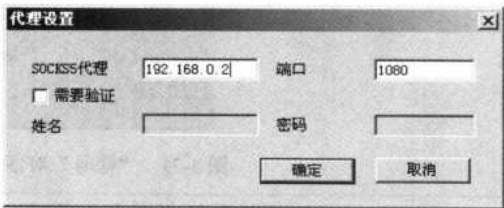


图 5-68 设置杀毒服务器地址及端口

如果出于安全考虑，还要对收、发的邮件进行杀毒，则要选择“邮件杀毒”复选框，然后单击激活的【杀毒设置】按钮，打开如图 5-69 所示的对话框。在这个对话框中可以设置邮件杀毒服务器地址及连接所用的端口。这个杀毒服务器可以不在本机，而在网络上的其他计算机中，端口号必须为 110。如果杀毒软件安装在本机服务器上，IP 地址可填写 127.0.0.1。

如果要启用邮件服务器的反垃圾邮件功能，则要选择“启动智能反垃圾邮件”复选项。被判断为垃圾邮件的邮件会自动存储到垃圾箱里，用户可以登录 Webmail 查看这些被屏蔽的垃圾邮件。如果还要配置允许邮箱账户发来的邮件，则单击随之激活的【反垃圾邮件设置】按钮，打开如图 5-70 所示的对话框。

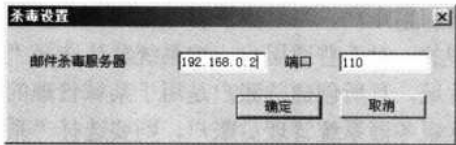


图 5-69 “杀毒设置”对话框

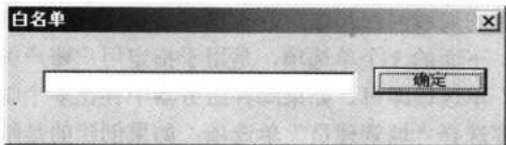


图 5-70 “白名单”对话框

“白名单”是指针对指定的域名或者 IP 地址不进行垃圾邮件检测。格式可以是：@topmail.com; 202.201.0; 203.202.1.2; 表示对于来自 topmail.com、202.201.0.1-202.201.0.255 及 203.202.1.2 的邮件不进行垃圾邮件检测。

5.7.2 邮箱账号创建与配置

此处介绍的账户创建方式同样适用于其他邮件服务器类型，后面不再介绍。CMailServer 提供了如下两种模式来实现邮箱账号创建方式。

1. 通过 CMailServer 操作界面创建

（1）在 CMailServer 的用户列表视图上单击鼠标右键，在弹出的快捷菜单中选择【新建账号】命令，打开如图 5-71 所示的对话框。

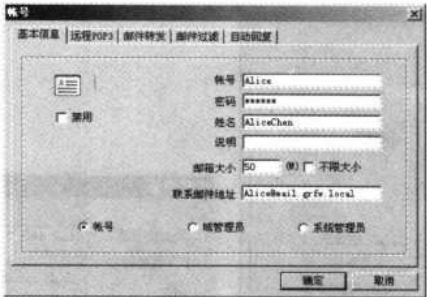


图 5-71 “账号”对话框“基本信息”选项卡



注意

邮件服务器程序在安装时就已自动创建了一个邮件服务器系统管理员账户 admin，所以，一般情况下不需要另外创建系统管理员账户了。但是管理员需要更改自己创建的系统管理员账户密码，否则很不安全，因为该账户的默认密码为空。该账户不能删除。

在“账号”和“密码”文本框中分别输入相应用户的基本账户名称和密码，它是用于在同一邮件域中直接使用的；在“姓名”和“说明”两文本框中可以不配置；在“邮箱大小”文本框中可设置该用户邮箱的大小，默认的是在如图 5-64 所示的对话框中设置的邮箱大小，在此可以任意更改，选择“不限大小”复选项，则该账户的邮箱大小不限。当然它不可能大过服务器所剩余的全部空间。

在“联系邮件地址”文本框中可以直接输入用于联系的任意一个邮箱账户，可以是这里配置的局域网邮箱账户，也可以是该用户的互联网邮箱账户，当然也可以不配置。

下面的 3 个单选项，是用于指定用户账户类型的，对于普通用户，按系统默认选择“账号”单选项即可。如果邮件服务器中存在多个邮件域，且所创建的账户是用于某域管理的，则要选择“域管理员”单选项；如果创建的是邮件服务器系统管理员账户，则要选择“系统管理员”单选项。

(2) 单击“远程 POP3”选项卡，如图 5-72 所示。在这里要设置通过 CMailServer 邮件服务器接收相应账户外网账户邮件的有关选项。因为此处配置的是局域网邮件服务器，所以此处可配置另一个邮件域的 POP3 邮件服务器中的邮箱账户。但在本章后面介绍的“局域网拨号邮件服务器”和“互联网邮件服务器”中，则此处可同时配置局域网和互联网邮箱账户。



图 5-72 “账号”对话框“远程 POP3”选项卡

首先要选择“允许 POP3 接收”选项，然后在下面配置外网用户邮箱账户的 POP3 服务器地址、所用端口（通常是 110，不用改）、账号和密码。通常此处的“账号”仅是邮箱地址“@”符号的前面部分，不过这里的“账号”也要区分不同的 POP3 账户类型，如果在对方邮件服务器上也有多个邮件域，则是整个邮箱账户地址。

如果要采取 SSL 安全连接，则要选择 SSL 复选项；如果想要在 CMailServer 邮件服务器上保留邮件副本，则选择“保留副本”复选项。

(3) 单击“邮件转发”选项卡，如图 5-73 所示。在如图 5-72 所示选项卡中设置的是接收其他局域网邮箱账户邮件的选项，而此步要设置的是通过 CMailServer 向外转发邮件的相关选项。



图 5-73 “账号”对话框“邮件转发”选项卡

这里的设置很简单，首先也是要选择“允许邮件转发”复选项，然后只需把要转发的目的邮箱账户（要求是完整的账户）添加到列表中即可。如果要在本地 CMailServer 邮件服务器上保留副本的话，则要选择“保留副本”复选项。

(4) 单击“邮件过滤”选项卡，如图 5-74 所示。在这里可以设置邮件过滤选项。邮件过滤的方式在其中有两种选项：一是通过邮件主题过滤；另一种是通过邮件发件人过滤。首先要选择“允许邮件过滤”复选项，如果要通过主题关键词过滤，则在“主题”下拉列表框中选择过滤的条件，然后在下面的文本框中输入要过滤的关键词；如果要通过邮件发件人来过滤，则在“发件人”下拉列表框中选择过滤的条件，然后在下面的文本框中输入要过滤的发件人邮件账户。最后通过单击【增加】按钮添加到过滤列表中即可。

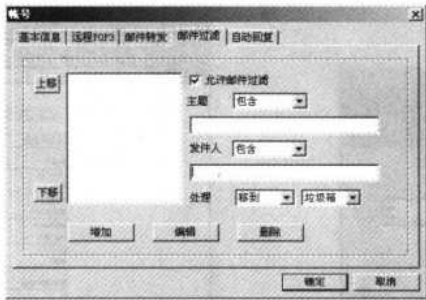


图 5-74 “账号”对话框“邮件过滤”选项卡

在下面的“处理”栏中可以选择当接收到符合以上条件的邮件时所采取的处理方式，可

以是移到垃圾邮箱中，也可以直接删除。

（5）单击“自动回复”选项卡，如图 5-75 所示。在这里可以设置当收到邮件后，用户通过邮件服务器自动发送的回复邮件。首先要选择“允许自动回复”复选项，然后在下面的“主题”和“内容”文本框中输入相应回复信件的主题和具体内容即可。

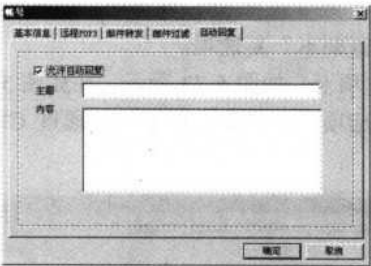


图 5-75 “账号”对话框“自动回复”选项卡

（6）所有需配置的选项设置好后，单击【确定】按钮后可完成一个用户账户的创建，其他账户的创建重复以上方法即可。

2. 通过 WebMail 由用户申请

以上是系统管理员在邮件服务器上为用户创建新账户的方法，在 CMailServer 中，客户端用户还可以通过如图 5-60 所示的 WebMail 界面自己申请，当然这要求系统已安装了 WebMail 功能，同时在如图 5-64 所示的选项卡中选择“允许通过网页申请账号”复选框。

方法很简单，用户自己申请账号的方法是在客户端的浏览器地址中输入：<http://邮件服务器IP地址（或邮件服务器计算机名）/mail>，如 <http://grfwgz-sl/mail>。需要注意的是，不是邮件服务器域名。如果在 IIS 默认网站上配置的是允许匿名访问，则可直接进入如图 5-60 所示的界面；如果 IIS 默认网站上配置的是不允许匿名访问，则首先弹出一个网站进入身份验证对话框，如图 5-76 所示。在这里要输入的是“默认网站”上允许访问的合法用户账户（此处要输入的不是邮件服务器上配置的用户账户，对应于不同的身份验证方式，一定要注意），然后单击【确定】按钮再进入到如图 5-60 所示界面。

直接单击如图 5-60 所示界面中“马上注册”链接进入到如图 5-77 所示的新用户信息配置对话框，输入方法与图 5-71 类似，输入好后单击【注册】按钮进行新用户注册即可。



图 5-76 进入 WebMail 网站的身份验证对话框



图 5-77 注册账户的 Web 界面

注册完成后，如果成功则显示如图 5-78 所示的提示。但最终是否可以立即使用，还要看如图 5-64 所示的选项卡中是否选择了“账号申请需要授权才能开通”复选项，如果选择了，用户申请后还需管理员授权批准，在 CMailServer 用户列中显示的相应用户状态为“禁用”，如图 5-79 所示。此时管理员要启用该账户的方法是直接在如图 5-79 所示用户列表中双击相应的用户，打开相应用户的属性对话框，参见图 5-71。不过，此时默认的是选择了“禁用”复选项，取消它的选择，然后单击【确定】按钮即可启用该账户了。如果在如图 5-64 所示的选项卡中没有选择“账号申请需要授权才能开通”复选项，则用户注册后，无须管理员再次授权，直接就可以使用了。

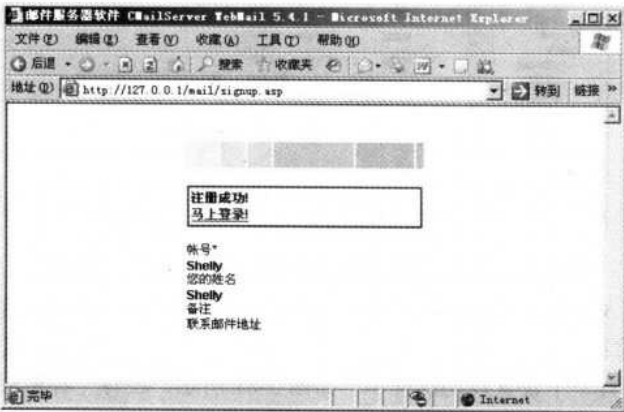


图 5-78 注册成功后的提示

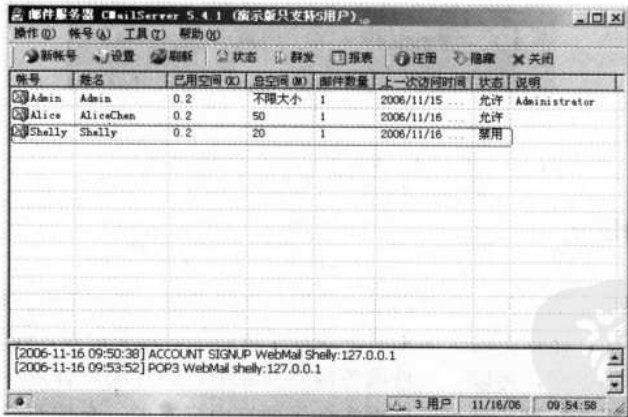


图 5-79 需要由管理员授权时客户申请账户的禁用状态

启用了的账户就可以通过单击如图 5-77 所示界面中的“马上登录”链接，返回到如图 5-60 所示界面（当然也可以直接在此界面中登录）。此时可以直接输入自己所申请的账户登录了。注册后的账户首先自动采用的是在 5.7.1 节基本配置中的设置。要改变设置，仍需由管理员根据前面介绍的方法在邮件服务器上设置。

登录后进入相应用户账户的 WebMail 界面，如图 5-80 所示。在这里可以进行许多像平时所使用的互联网邮箱类似的操作功能，如收、发、查看邮件，整理邮箱中的邮件，还可自

300 网管员必读——网络应用（第 2 版）

已修改账户设置等。

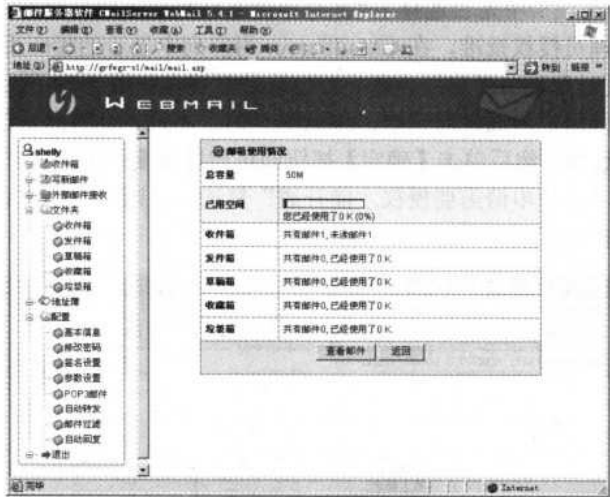


图 5-80 WebMail 首页

如果访问不了 WebMail 界面，通常是因为 IIS 不稳定造成的。建议重新安装操作系统和 IIS，并打上相应的补丁。然后在 CMailServer 主界面中执行【工具】→【设置虚拟目录】菜单操作，完成后会有一个设置成功的提示，如图 5-81 所示。还有一种可能，服务器上安装了某些杀毒软件，需要关闭这些杀毒软件中的脚本监视功能。

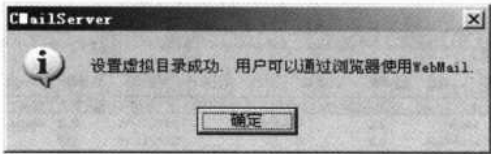


图 5-81 设置虚拟目录成功提示框

5.7.3 用户组的建立

除了可以创建单个用户外，还可创建用户组，以便管理。方法是在如图 5-79 所示的程序主界面单击鼠标右键，在弹出的快捷菜单中选择【新建邮件组】命令，打开如图 5-82 所示的对话框。在这个对话框中，可以把邮件服务器当前域中已创建的所有用户选择性地加入到新用户组中。用户分组的标准当然可以根据实际需要自由定义了，有按部门的，有按职务的，也有按工作性质的，当然也可以根据临时应用需求来创建。这样当向组账户中发送邮件时，则邮件会自动分发到组中的所有成员邮箱中，实际就相当于邮件群发功能。

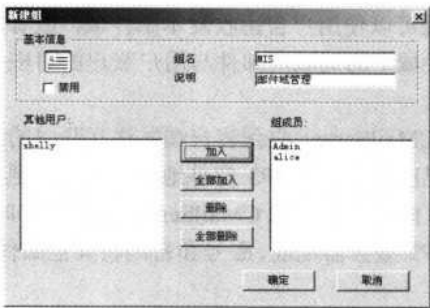


图 5-82 “新建组”对话框

如果要把所有用户添加到某个组中（如要向公司所有员工发送消息），则可直接单击【全部加入】按钮，即可把“其他用户”列表中的用户全部添加到“组成员”列表中，成为组成员。要删除组成员中的账户可以选择在“组成员”列表中的相应用户（可通过按住【Shift】键连续多选，或者按住【Ctrl】键非连续多选），然后单击【删除】按钮；如果要删除组成员中的所有成员，则单击【全部删除】按钮即可。

5.7.4 客户端 Outlook Express 的配置

用户账户申请好以后，就要配置客户端 Outlook（包括 Outlook Express，OE）了，下面以 Outlook Express 6.0（简称为 OE 6.0）为例进行内外部邮件收发配置。OE 中的设置也非常简单，只需在“服务器”选项卡中进行必要的配置即可，如图 5-83 所示。

在这里的配置中，要注意的是 POP3 和 SMTP 服务器的配置，此处要指向 CMailServer 邮件服务器的实际 IP 地址，或计算机名；而在其中的“账户名”文本框中，在 CMailServer 邮件服务器中，只有一个邮件域的时候，则仅需要输入相应用户账户名即可，而不用输入完整的用户邮箱账户，也就是不用输入邮件域尾缀。

如果发送邮件时需要验证用户身份，则要求选择“我的服务器要求身份验证”复选框。当然，同时也需在如图 5-62 所示的对话框中选择“允许 ESMTP”复选框。

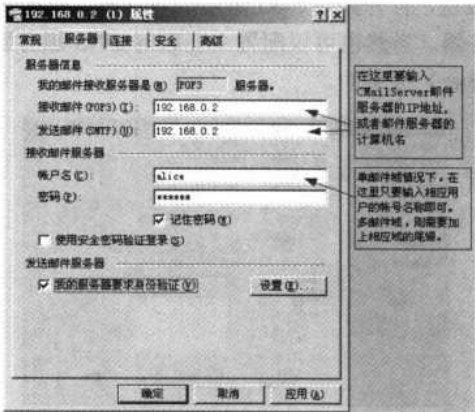


图 5-83 “服务器”选项卡

302 网管员必读——网络应用（第2版）

通过以上简单的设置就可以使用户自由收发本邮件域，或者其他邮件域中的局域网邮箱账户邮件了，因为其他邮件域中的局域网邮件与用户账户的对应关系已在用户账户申请时配置，参见图 5-71 和图 5-72。

具体实现原理是：当 CMailServer 收到客户端发往互联网的邮件时，就会自动将邮件中的本地邮箱地址替换成自己所设置的 POP3 邮件地址，然后再通过 CMailServer 的邮件发送程序发送到其他邮件域中。而客户端登录 CMailServer 收取邮件时，CMailServer 又会根据该用户提供的其他域中的 POP3 服务器地址、账号和密码将其他邮件域中的邮件收回本地邮箱。

5.8 其他类型邮件服务器建立与配置

CMailServer 除了可以配置局域网邮件服务器，还可以配置互联网邮件服务器、局域网+拨号邮件服务器和多域邮件服务器。因为大多数选项的配置与前面介绍的局域网邮件服务器的设置方法一样，所以下面仅对一些不同之处进行介绍。

5.8.1 互联网邮件服务器建立与配置

将 CMailServer 作为互联网邮件服务器，必须具备如下的条件。

- 拥有一台运行在互联网上的服务器，有固定的互联网 IP 地址，将 CMailServer 安装在这台机器上。
- 拥有一个互联网合法域名（假设为 grfw.com），那么你的邮件地址格式就是 user@grfw.com。SMTP 地址和 POP3 地址就是服务器对应的互联网地址。
- 与你的互联网域名服务提供商联系，将你的域名的 MX 记录设置成服务器对应的互联网地址。

具体操作步骤如下。

（1）在如图 5-62 所示的对话框中选择“作为互联网邮件服务器”单选项，然后在“单域名”（在此仅以单域名为例进行介绍）文本框中输入在互联网已注册的域名。如图 5-84 所示。

（2）单击【高级】按钮，打开如图 5-85 所示的对话框。在这里要指定“主互联网 DNS”和“副互联网 DNS”服务器。当然也可仅配置主互联网 DNS 服务器，这两个 DNS 服务器一般都是由 NSP（网络服务商）提供的。

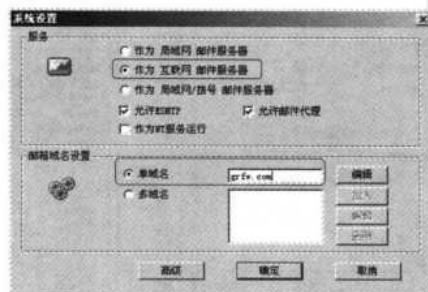


图 5-84 创建互联网邮件服务器时选择



图 5-85 创建互联网邮件服务器时的 DNS 服务器配置

在如图 5-85 所示的对话框中的其他选项卡配置均可参照前面介绍的局域网邮件服务器的配置。只是在“邮件过滤”选项卡（参见图 5-66）中可以配置要过滤的互联网邮件和 IP 地址。

（3）再配置具体用户账户。在 CMailServer 主界面中单击鼠标右键，在弹出的快捷菜单中选择【新建账户】命令，打开如图 5-71 所示的对话框。在这里要配置用户的互联网邮箱账户，而不再是局域网账户。同样，在如图 5-72 “远程 POP3”和图 5-73 “邮件转发”所示的两个选项卡中，配置该用户可以收、发来自互联网邮件的邮箱账户。在如图 5-74 所示的“邮件过滤”选项卡中可以配置要过滤的互联网邮件主题和发信人账户。在如图 5-75 所示的“自动回复”选项卡中同样可以配置该用户回复互联网账户邮件的自动回复信件。

至于客户端的邮箱账户配置就与我们平常所用的互联网邮箱账户配置完全一样，不再赘述。只不过所配置的 POP3 和 SMTP 服务器地址要指向自己创建的邮件服务器地址。



如果你的公司没有固定的互联网 IP 地址，而仅有互联网域名，且要架设互联网邮件服务器，则同样需要用到 DDNS（动态域名服务）了。同样需要借助于动态域解析服务，并在相应动态域名中添加指向邮件服务器的 MX 记录。具体在第 1 章中已有详细介绍，参见即可。

5.8.2 局域网拨号邮件服务器

大部分公司没有一个拥有互联网固定 IP 的服务器，但是随着宽带的应用，大部分公司都可以有一台常年包月上网的服务器，而且公司已经在互联网上拥有了自己的邮箱空间（一般都是域名服务商提供的）。域名服务商提供的邮箱空间有几个缺陷：本公司发送到本公司邮箱也经过互联网，这样发送速度非常慢；不方便邮件管理和邮件监控；收发邮件时总是要连接互联网，邮件下载速度慢。这些问题，在 CMailServer 局域网拨号邮件服务器里都得到了很好的解决。这是目前在企业中应用最多的一种邮件服务器类型。它主要用于局域网邮件通信，同时又能收发互联网邮件。

局域网拨号邮件服务器的工作原理是这样的，邮件首先发送到 CMailServer 里，然后 CMailServer 再将邮件发送到互联网。同时，CMailServer 开启了多个线程，把互联网上的邮件下载到本地邮箱。

局域网拨号邮件服务器的具体配置方法也与局域网邮件服务器的配置方法差不多，下面也仅介绍不同之处。

304 网管员必读——网络应用（第2版）

(1) 在如图 5-84 所示的对话框中选择“作为局域网/拨号邮件服务器”单选项，然后在“单域名”（在此仅以单域名为例）文本框中输入邮件服务器的域名。这里的域名既可以是局域网的，也可以是互联网上的，实际上它是一个虚拟域名。

(2) 创建并配置用户账户。在如图 5-72 所示选项卡中，同样可以任意配置用户名、密码及邮箱大小等信息。但在这里，在“联系邮件地址”文本框中一定要为用户指定一个有效的互联网邮箱账户，如图 5-86 所示。

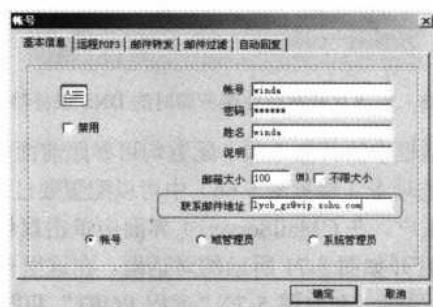


图 5-86 配置局域网拨号邮件服务器用户账户时必须指定联系邮件地址

这是因为如果服务器设置的邮箱域名是虚拟的（并不是互联网中有效的域名），互联网是无法识别的，对方无法正常回复邮件，所以还要在客户端申请邮箱时提供一个有效的互联网邮箱来作为中转邮箱。当 CMailServer 收到客户端发往互联网的邮件时，会自动将邮件中的虚拟邮箱地址替换成自己所设置的“联系邮件地址”，然后再通过 CMailServer 的邮件发送程序发送到互联网。当对方收到邮件后，就会将邮件回复到这个“联系邮件地址”。而客户端登录 CMailServer 收取邮件时，CMailServer 又会根据该用户提供的 POP3 服务器地址、账号和密码将对方的回复邮件收到本地邮箱中。

(3) 在如图 5-72 “远程 POP3” 和图 5-73 “邮件转发” 所示的两个选项卡中，配置该用户可以收、发来自其他局域网邮件域，或者互联网的邮箱账户。在如图 5-74 所示的“邮件过滤”选项卡中可以配置要过滤的局域网邮件域，或者互联网邮箱主题和发信人账户。在如图 5-75 所示的“自动回复”选项卡中同样可以配置该用户账户回复局域网邮件域，或者互联网邮件的自动回复信件。

至于客户端的邮件程序配置与局域网邮件服务器的配置完全一样。

5.8.3 多域名邮件服务器建立与配置

多域名服务器和单域名服务器的设置大部分都是一样的。只是在域名设置和账号设置里，有一些不同。需在如图 5-84 所示的对话框中选择一种邮件服务器类型后，然后再选择“多域名”单选项，再依次添加多域名。然后再为每个邮件域按前面介绍的对应邮件服务器类型配置方法进行配置即可。当然所添加的多个域名必须与所选的邮件服务器类型一致，不能混合添加局域网和互联网邮件域。

另外，在创建邮件服务器用户账户时，在如图 5-72 所示的对话框中就不能只输入用户名，而应输入包括邮件域名的完整的用户邮箱账户。如在单域名模式下，邮件地址是

user@grfw.com，登录账号是 user；在多域名模式下，邮件地址是 user@grfw.com，登录账号却必须是 user@grfw.com，不能省略后面的邮件域名后缀。这一点在邮件服务器中创建了多个邮件域时一定要注意到。



从以上几种邮件服务器类型的建立与配置过程可以看出，这几种邮件服务器存在着相当大的共同配置，所以在要转换邮件服务器类型时，无须全部重来，可以直接通过在如图 5-84 所示的对话框中选择另一种邮件服务器类型，然后再按照 5.8 节介绍的对应邮件服务器类型配置的不同之处重新配置一下即可实现邮件服务器类型的轻松转换。

5.9 CMailServer 邮件服务器的维护与管理

CMailServer 的功能总体来说还是相当不错的，特别适用于中小型企业。本节要向大家介绍的是这款邮件服务器系统的基本维护和管理方法。

5.9.1 CMailServer 企业邮局的维护

在使用 CMailServer 的过程中的确也发现了一些问题。不过，许多问题都可以通过远志公司提供的帮助文档加以解决。下面是一些常见问题的解决方法。

1. 问：为什么邮件服务器不能向外发邮件？

答：以下原因都可能导致无法发送邮件。

(1) 检查一下所配置的邮件服务器是否具有互联网邮件发送功能，也就是“局域网拨号邮件服务器”，或者“互联网邮件服务器”类型，如果是“局域网拨号邮件服务器”类型，则不能向外发送互联网邮件。如果用局域网邮件服务器来向外发送邮件，会得到如图 5-87 所示错误提示，提示中说明当前服务器为局域网（LAN）邮件服务器，不能向外转发邮件。如果是局域网拨号邮件服务器，在按照本章前面介绍的配置方法配置好后，很容易向外发送互联网邮件，如图 5-88 就是笔者通过局域网拨号邮件服务器的内部账户向互联网邮箱 lymb_gz@vip.sohu.com 发送的一份测试邮件。

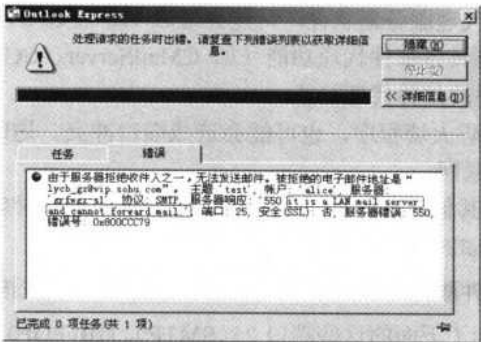


图 5-87 用局域网邮件服务器向外发送互联网邮件时的错误提示



图 5-88 利用局域网拨号邮件服务器发送互联网邮件的测试邮件

(2) 检查服务器上是否安装了防火墙软件，如果安装了，需要开放 25、110、5353、80、53 端口，需要允许 CMailServer 完全访问互联网，需要允许 IIS、dllhost.exe 完全访问互联网。如果不知道怎么操作防火墙软件，最好在关闭防火墙的情况下测试 CMailServer。

(3) 检查服务器上是否安装了杀毒软件，如果安装了，需要关闭该杀毒软件的邮件监视功能，因为它们占用了 25 号端口。

(4) 如果本地无法 ping 通互联网根域名服务器 a.root-servers.net 和 b.root-servers.net，需要在如图 5-85 所示选项卡中填上两个本地电信提供的 DNS 地址。

2. 问：CMailServer 和 CCProxy（或其他代理服务器）安装到同一台机器时，需要注意什么？

答：取消 CCProxy 设置里的“邮件代理”选项，因为 CMailServer 已经有邮件代理功能了。

3. 问：为什么会出现 SMTP 或者 POP3 服务启动失败？

答：这是因为你的服务器上安装了其他与邮件服务有关的程序，造成端口冲突。有很多原因可导致这种现象。

(1) 如果你安装了可以防止 E-mail 病毒的杀毒软件，你需要的杀毒软件的邮件监视功能可能会造成 110（POP3）端口冲突。如果依然不能解决，那就只有反安装该杀毒软件，改用其他杀毒软件，CMailServer 与 Norton 杀毒软件完全兼容。

(2) 如果你安装了代理服务器软件，可能会造成 110（POP3）、25（SMTP）端口冲突。因为有些代理服务器可能具备邮件代理功能（如 CMailServer、CCProxy）。在这种情况下，你需要停止代理服务器中的邮件代理功能。

(3) 如果你安装了防火墙程序，也可能造成端口冲突。这时需要设置防火墙，允许 CMailServer 完全访问互联网。

(4) 如果你安装了其他的邮件服务器程序，也会造成端口冲突。必须停止并反安装这些邮件服务器才能使 CMailServer 运行正常。

4. 问：如果我的邮件服务器安装了严格的防火墙控制，我应该开放哪些端口？

答：CMailServer 用到了下面的这些端口 25（SMTP）、110（POP3）、53（DNS）、80（HTTP）、8011（Admin）、5353（MX），CMailServer 要求防火墙开放这些端口。

5. 问：怎样限制 WebMail 附件大小发送和单个邮件大小？

答：按如下步骤配置。

(1) 打开 CmailServer 程序安装目录中的 WebMail 子目录。

(2) 找到并用写字板，甚至记事程序打开 postmail.asp 文件，然后修改第 33 行：
'nMaxMailSize = 2 * 1024 * 1024。

(3) 去掉那个单引号，就可以限制附件大小了。默认是 2*1024*1024=2MB，可以改成任意大小，单位是字节。如果希望限制单个邮件大小，可以修改 CmailServer 安装程序根目录 config.ini 文件中的 MaxMailSize 值。单位为字节。

6. 问：为什么发送邮件或者转发邮件，附件不能下载？

答：将 CmailServer 安装程序主目录的安全属性设置成对 everyone 可读可写。然后在主界面中执行【工具】→【设置虚拟目录】菜单操作，系统会自动在 IIS 默认网站中把用户邮箱目录添加为虚拟目录。

7. 问：为什么发送邮件时经常会出现“ERR 550 mail server cannot forward...”？

答：这是因为你将邮件服务器设置成了“作为局域网拨号邮件服务器”，你要在账号设置里提供一个有效的 POP3 邮件地址，才能发送互联网邮件。比如你可以通过 WebMail 登录后，选择“设置”，在“POP3 邮件地址”栏填上一个你常用的互联网 E-mail 地址，并设置对应的 POP3 密码和 POP3 服务器地址，就可以收别人发给你的邮件了。

8. 问：怎样防止非法用户使用邮件服务器发送垃圾邮件？

答：需要在设置对话框中选择“允许 ESMTP”复选框，取消选择“允许邮件转发”复选框。在客户端的 OE 设置中要选择“邮件发送验证”复选框。

9. 问：为什么发送一封很多收件人的邮件时，会出现 too many receivers？

答：这是因为 CMailServer 有最多收件人限制，可以在程序安装目录用记事本程序打开 config.ini 文件，将其中的 MaxRcpt=20（表示最多填写 20 个收件人地址，这里的收件人数其实包括“收件人”、“抄送人”和“暗送人”总数）修改成所需要的数字后，重启 CMailServer 即改变成你所设定的值了。

10. 问：为什么服务器总是不停地发送同一封邮件，导致用户收到多封相同的邮件？

答：这是因为服务器上安装的杀毒软件的邮件监视功能引起的，请停止服务器杀毒软件的邮件监视功能。

11. 问：为什么邮件服务器接收不到邮件？

答：可以从下面这些方面去分析一下。

(1) 检查服务器上是否安装了防火墙软件，如果安装了，需要开放 25 端口，需要允许 CMailServer 完全访问互联网。检测 25 端口是否开放，可以在外网用 telnet 命令来检测。假设你的域名是 210.0.0.1，你可以用 telnet 210.0.0.1 25 来测试。如果开放了，服务器会返回“220...”字样。

(2) 检查服务器域名的 MX 记录是否设置正确。可以用这样的方法检测。在命令行里输入 nslookup 命令，然后输入 settype = mx 后回车，然后再输入自己的邮件域名后回车，就可以看到 MX 记录是否设置成功，即是否指向了邮件服务器的地址。如果没有设置正确，需

308 网管员必读——网络应用（第2版）

要联系域名提供商，要求他们进行修改。

（3）有些防病毒软件因为截获了发送的邮件，会导致无法发送邮件。可以试着关闭防病毒软件里的邮件发送监控功能看看。

（4）在这里下载在线检测工具：<http://www.yzsoft.com/mailcheck.php>。

12. 问：怎样用匿名账号发送邮件？

答：在某些特殊情况下，需要让特定 IP 的客户端可以用匿名账号发送，不通过验证来发送邮件。设置方法是打开程序安装根目录下的 config.ini 文件，设置 PermittedIPSMTP 和 AnonymousAccount 这两个参数。PermittedIPSMTP 是允许进行匿名发送的客户端 IP 地址，如果多个 IP，可以用分号分割多个 IP。AnonymousAccount 是默认的发件人地址（在与目标邮件服务器通信时的发件人地址），这个地址可以是不存在的，但是需要是本地域名。比如你的邮件服务器域名是 a.com，可以设置 anonymouse@a.com 作为 AnonymousAccount 账户。

其实在 CMailServer 还有一个包含所有用户的组，那就是 all，如果对应的邮件域名为 a.com，则它对应的账户就是 all@a.com。利用这个账户可以向所有用户发送消息，这样一来，就不能在邮件域中建立一个与“all”同名的用户组了，使用时一定要注意。

5.9.2 CMailServer 邮件服务器的基本管理

在 CMailServer 邮件服务器中提供了非常丰富的服务器管理功能，下面介绍几个主要的服务器管理功能。

1. 账户密码修改

此处包括管理员和普通用户账户密码的修改。管理员密码的修改是在 CMailServer 程序主界面中执行【工具】→【管理员密码】菜单操作，打开如图 5-89 所示的“修改密码”对话框。在此对话框的对应选项中输入新、旧密码，然后单击【确定】按钮即可完成管理员密码的修改。

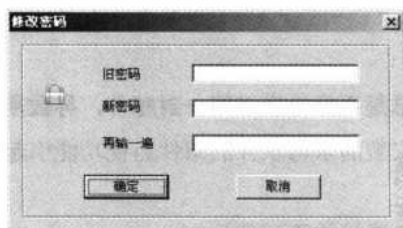


图 5-89 “修改密码”对话框

用户密码的修改可由管理员直接在相应账户上单击鼠标右键，在打开的如图 5-86 所示的对话框中修改。

2. 编辑用户欢迎信

管理员可以在服务器中编辑用户第一次使用 CMailServer 邮件系统时所收到的欢迎邮件。方法是在 CMailServer 程序主界面中执行【工具】→【编辑欢迎信】菜单操作，打开如图 5-90 所示的对话框。在其中就可以编辑欢迎信的发信人账户（通常为系统管理员）、主题、内容，

至于接收邮件用户名则不用更改，它是针对所有新用户的。

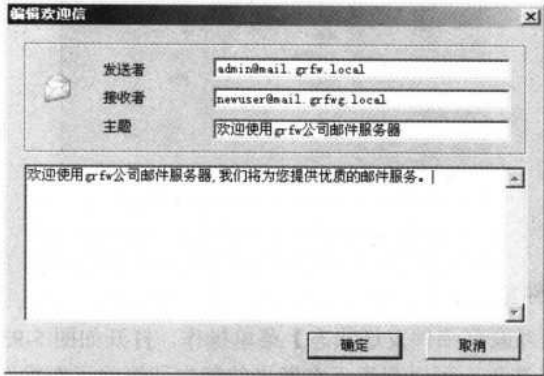


图 5-90 “编辑欢迎信”对话框

3. 群发邮件

当管理员认为有必要对所有用户发邮件时，可以利用服务器的此项功能。方法是单击 CMailServer 程序主界面工具栏中的【群发】按钮，打开如图 5-91 所示的“发送邮件”对话框。在此对话框中的邮件的接收者为所有服务器邮箱用户（默认为“ALL”账户，表示所有用户，是一个系统内置组账户，也可以在此输入用户组账户）。还可以添加附件，方法是通过单击【增加附件】按钮，打开一个对话框进行选择。输入好内容后单击【发送邮件】按钮，即可把邮件发送到指定所有用户邮箱中。

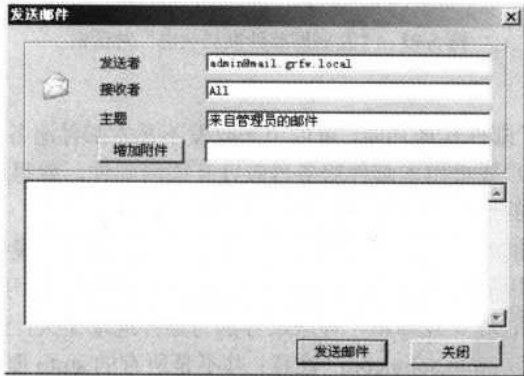


图 5-91 “发送邮件”对话框

4. 生成管理报表

当服务器长期运行时，通常需要对一定时间的用户邮箱使用情况进行检查，此时这项报表功能就相当有用了。通过单击 CMailServer 程序主界面工具栏的【报表】按钮，打开如图 5-92 所示的“输出用户信息”对话框。在这个对话框中可以选择报表所需输出的信息选项，相当于数据库字段和报表输出格式。

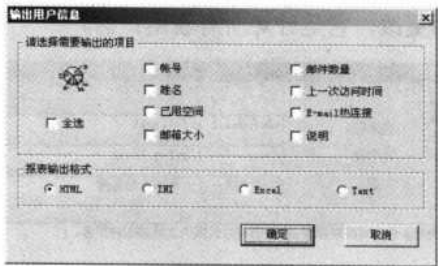


图 5-92 “输出用户信息”对话框

5. 查看互联网邮件发送状态

执行【工具】→【互联网邮件发送状态】菜单操作，打开如图 5-93 所示的对话框。选择“正在发送的邮件”单选项，可以观察正在发送的邮件和删除正在发送的邮件；选择“无法传递的邮件”单选项，可以观察无法传递的邮件信息，可以重发和删除这些无法传递的邮件。



图 5-93 “互联网邮件发送状态”对话框

6. 邮件代理

CMailServer 内置了邮件代理功能，可以用来收发不是本邮件服务器域的互联网邮件。也就是其他邮件域中的账户要借用本邮件服务器收发互联网邮件，就得启用 CMailServer 的邮件代理功能。这一功能的设置参见图 5-67 和图 5-68。

除了要启用代理功能外，还要在客户端的邮件程序中进行账户设置。以 OE 为例。

假设要代理收发的用户邮箱地址：lycb@sohu.com；假设邮箱账号：lycb（注意：有的账号是完整的 E-mail 地址，如企业邮箱，有些账号则与邮件地址无关，请根据自己邮箱的情况设置）；假设 SMTP 地址：smtp.sohu.com（注意：并不是所有的 smtp 服务器地址都是 smtp.* 格式，请根据自己邮箱的情况设置）；假设 POP3 地址：pop3.sohu.com（注意：并不是所有的 POP3 服务器地址都是 pop3.* 格式，请根据自己邮箱的情况设置）；假设 CMailServer 服务器地址：192.168.0.2。那么在 OE 里可以进行如下修改：

邮箱账号：lycb#pop.sohu.com；SMTP 地址：192.168.0.2；POP3 地址：192.168.0.2；发送服务器设置：账户名为 lychb#smtp.sohu.com（如果原邮件服务器不需要发送验证，账号名为#smtp.sohu.com）。

至于像邮件服务器的启用、停止和用户账户的管理方法都很简单，通常只需通过鼠标右键快捷菜单进行即可，为了节省篇幅，在此不作具体介绍。另外，管理员还可通过 WebMail 进行远程管理，远程管理的方法在本章前面已有介绍，在此不再赘述。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

CHAPTER

6

第 6 章 大中型企业邮局系统

在第 5 章介绍了 Windows Server 2003 系统中的 POP3 和 CMailServer 两款适合于中小企业的邮件服务器组建方法，本章要介绍适合于大中型企业局域网的企业邮局——Exchange Server 2003 系统企业邮局的组建方法。

相对于第 5 章介绍的 POP3 邮件系统，本章所要介绍的 Exchange Server 2003 系统企业邮局无论是在配置上，还是功能上都有相当大的区别。Exchange Server 2003 系统是一个技术非常复杂的大型邮件服务器系统，包括了非常多的功能，配置也相当复杂。出于篇幅的考虑，本章主要介绍 Exchange Server 2003 邮件服务器系统的典型配置方法与步骤，在技术方面，只在一些关键技术配置时作简要的说明，不作深入的介绍，因为本书主要介绍的是应用方法，而不是技术原理。如需全面了解这一大型邮件服务器系统技术，请参见其他相关资料。

本章重点

- 安装 Exchange Server 2003 的条件和 8 个步骤
- Exchange Server 2003 服务器全局节点设置方法
- Exchange Server 2003 服务器属性设置方法
- 公用文件夹、公用文件夹存储的创建与配置
- 邮箱存储的创建与配置
- 用户、组邮箱的创建与配置
- “邮箱存储”和“收件人”策略的创建与管理
- 地址列表的创建与配置
- SMTP 虚拟服务器的配置
- Outlook 2003 客户端 Exchange 电子邮件账户的创建与配置
- 邮件服务器的常规管理方法

6.1 Exchange Server 2003 简介

Microsoft 的 Exchange Server 就像其操作系统一样，也经过了好几个版本的发展，目前主流应用的版本仍为 Exchange 2000 和 Exchange Server 2003 两个版本，尽管它的最新版本 Exchange Server 2007 已经发布。

目前，Exchange Server 2003 最新补丁为 SP2，它在功能上和安全措施上都有许多增强。有关 Exchange Server 2003 和其 SP2 补丁的新增功能和功能改进所涉及的内容太多，在此不作具体介绍，可以参考 Microsoft 公司的官方网站：<http://www.microsoft.com/technet/prodtechnol/exchange/zh-cn/guides/WhatNewE2k3/aa9bc812-6f7f-4892-8bf0-06f5eff204bb.mspx?mfr=true>。本章也是以其安装了最新补丁 SP2 后的系统进行介绍的。

6.1.1 Exchange Server 2003 的两个版本

Exchange Server 2003 有两个版本：Exchange Server 2003 企业版和 Exchange Server 2003 标准版。Exchange Server 2003 企业版相对于标准版来说包括了下列增强功能。

- 支持多达 4 个存储组，每个存储组最多可以容纳 5 个数据库。
- 数据库大小只受硬件限制（最大为 16 TB）。
- 可以通过 Microsoft Cluster Server 群集服务，将 Exchange Server 2003 企业版组成群集。
- 包括 X.400 连接器。

而 Exchange Server 2003 标准版存在以下局限性。

- 只支持一个存储组，且该存储组只能容纳两个数据库。
- 每个数据库最大不能超过 16GB。
- 不支持通过 Microsoft Cluster Server 群集服务组成群集。
- 不包括 X.400 连接器。

识别当前安装的版本是何版本的方法如下。

（1）执行【开始】→【程序】→【Microsoft Exchange】→【系统管理器】菜单操作，打开如图 6-1 所示的 Exchange Server 2003 控制台主窗口。

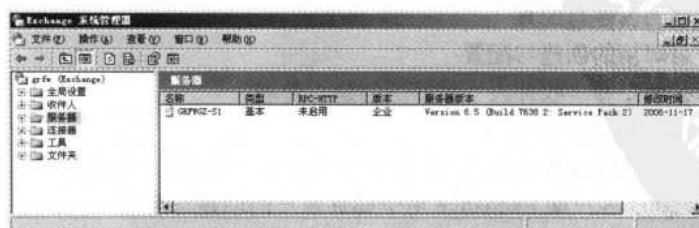


图 6-1 Exchange Server 2003 系统管理器界面

（2）在左列的控制台树中选择“服务器”容器选项，在右边的详细信息窗口中就列出了 Exchange 组织中的服务器的有关信息。

“版本”列显示服务器运行的是标准版还是企业版（对于 Exchange 5.5 服务器，始终显示“标准”，即使它们运行的是 Exchange Server 5.5 企业版），“服务器版本”列显示出安装的 Exchange 的版本号及内部版本号和安装的所有 Service Pack（补丁）。安装了 SP2 的 Exchange Server 2003 的版本号仍显示为 6.5，但会在后面的小括号中说明所安装的补丁为 SP2（Service Pack 2）。

6.1.2 Exchange Server 2003 支持的环境

Exchange Server 2003 不可以随便安装，它对网络系统平台要求还是相当严格的，在选购和部署时一定要注意，否则可能选购的软件不能在本企业财贸系统中使用。

Exchange Server 2003 可以在 Windows Server 2003 和 Windows 2000 Server SP3 或更高版本上运行。Exchange Server 2003 已经过优化，可以在 Windows Server 2003 平台上运行，有几项 Exchange Server 2003 功能要求必须是 Windows Server 2003 系统。所有 Active Directory 目录服务目录林环境都支持 Exchange Server 2003，其中就包括：纯 Windows 2000 目录林、纯 Windows 2003 目录林，以及混合的 Windows 2000 和 Windows 2003 目录林。



虽然包含 Windows Server 2003 域控制器和全局编录服务器的环境支持 Exchange 2000 SP2 和更高版本，但是 Windows Server 2003 支持运行的第一个 Exchange 版本是 Exchange Server 2003。Windows Server 2003 不支持 Exchange 2000 邮件系统。

当在包含 Windows 2000 域控制器和全局编录服务器的环境中运行时，Exchange Server 2003 使用的域控制器和全局编录服务器必须运行 Windows 2000 Service Pack 3 或更高版本。Exchange Server 2003 将不会使用未运行 Windows 2000 Service Pack 3 或更高版本的 Windows 2000 域控制器或全局编录服务器。此要求会影响到 Exchange Server 2003 服务器和 Exchange Server 2003 版的 Active Directory 连接器（ADC）。ADC 将不能与运行 Windows 2000 Service Pack 3 之前版本的域控制器或全局编录服务器协作工作。

Exchange 系统管理器、Active Directory 用户和计算机，以及其他管理工具不会筛选掉 Windows 2000 Server 的先前版本。为了确保与 Exchange 系统管理器和其他管理工具进行签名和封装的轻型目录访问协议（LDAP）通信，Active Directory 环境中的所有域控制器和全局编录服务器必须运行 Windows 2000 Service Pack 3 或更高版本。

如果在 Exchange 系统管理器上的“目录访问”选项卡中手动设置了未运行 Windows 2000 Service Pack 3 或更高版本的域控制器或全局编录服务器，Exchange 将不会使用该域控制器或全局编录服务器。

6.1.3 Exchange Server 2003 技术概述

1. Exchange Server 2003 的主要功能

作为邮件服务器平台，Exchange Server 2003 具有与其他电子邮件系统相同的下列功能。

- 无论预期的收件人驻留在本地服务器上，同一个 Exchange Server 2003 组织中的另一台服务器上，还是连接到组织的外部邮件环境中的另一台服务器上，都能够以可

314 网管员必读——网络应用（第2版）

靠的方式将电子邮件传输到该收件人。

- 在基于服务器的存储中存储电子邮件。
- 支持用于访问或下载邮件的各个电子邮件客户端。
- 通过通信簿或全局地址列表为用户提供组织中的收件人信息。

Exchange Server 2003 具有上述功能及其他许多功能。但是，Exchange Server 2003 自身不提供这些功能。Exchange Server 2003 与 Windows Server 2003 所提供的 TCP/IP 基础结构及 Active Directory 目录服务紧密集成。要了解 Exchange Server 2003 体系结构，必须首先了解与 TCP/IP 有关的技术，以及 Windows Server 2003 和 Active Directory。

此外，还必须熟悉下列通用的邮件概念（这些技术因篇幅的原因，在此不能一一介绍，需要的朋友，可以参考其他相关资料）。

- 邮件系统特征：了解邮件系统的典型组件及服务器之间的基本邮件流。
- Active Directory 与 Exchange Server 2003 的集成：了解 Exchange Server 2003 如何使用 Active Directory 来实现必要的目录基础结构。
- 邮件连接性：了解 Exchange Server 2003 如何将邮件从发件人传输到收件人。
- 邮件存储：了解邮件存储在邮件系统中的角色和用途。
- 支持的电子邮件客户端：了解可以用在 Exchange Server 2003 组织中的各个客户端和邮件访问协议。

2. Exchange Server 2003 的主要组成

所有的邮件环境都具有几个共同的典型要求。邮件环境中的每个邮件系统都至少需要具备以下条件。

- 邮件传输机制。
- 包含邮件系统中的所有用户的列表。
- 用于在客户端检索邮件之前存储邮件的位置。
- 可供电子邮件客户端用来与邮件环境中的服务器通信的接口。

Exchange Server 2003 包括了下列邮件组件。

1) 目录

目录包含有关系统用户的信息。此信息用于将邮件传递给预期的用户。该目录还存储有关邮件处理系统的大部分配置信息。其中包括有关系统配置的信息以及有关如何将邮件从一个邮件服务器路由到另一个邮件服务器的信息。在 Exchange Server 2003 中，该目录由 Active Directory 提供。Exchange Server 2003 中的许多组件都使用名为 DSAccess 的目录访问模块与 Active Directory 通信。



在 Exchange Server 2003 系统安装后也会在邮件服务器程序菜单中生成一个【Active Directory 用户和计算机】管理单元快捷项，这样就为管理员直接在邮件服务器上对用户至上、组等对象的管理提供了方便，并不是多余。因为邮件服务器通常不是在域控制器中安装的。

2) 邮件传输子系统

该组件实现电子邮件的路由和传输机制。邮件可能发往同一服务器上的收件人，也可能发往同一组织中的另一台服务器上的收件人，或者发往 Internet 或其他邮件系统中的收件人。

Exchange Server 2003 中的中心传输引擎是简单邮件传输协议（SMTP）传输引擎，该引擎在最初由 Windows Server 2003 IIS 提供的 SMTP 服务中实现。Exchange Server 2003 扩展了 SMTP 服务，以实现 Exchange Server 2003 需要的邮件处理功能。Exchange Server 2003 中的邮件传输完全依赖于 SMTP 传输引擎，即便发件人和收件人驻留在同一台服务器上也是如此。

3) 邮件存储

在 Exchange Server 2003 中，邮件存储（Exchange 存储）在邮箱和公用文件夹中存储电子邮件、邮件表和其他项目。当邮件从一台服务器路由到另一台服务器时，传输子系统使用该表来临时存储邮件。Exchange 存储依赖可扩展存储引擎（ESE）技术实现邮件数据库。

4) 用户代理

用户通过用户代理访问邮件系统。用户代理实际上就是邮件客户端。Exchange Server 2003 支持多种不同的邮件客户端，其中包括 MAPI 客户端、HTTP 客户端，以及使用 POP3、IMAP4 和网络新闻传输协议（NNTP）的客户端。另一方面，支持目录查找的轻型目录访问协议（LDAP）由 Active Directory 提供。

3. Exchange Server 2003 需要的网络组件

要在 Exchange Server 2003 组织中将邮件从一台服务器传输到另一台服务器，网络必须支持 TCP/IP。Active Directory 和 SMTP 服务都需要 TCP/IP。图 6-2 说明了实现系统通信和邮件传输所必需的组件。

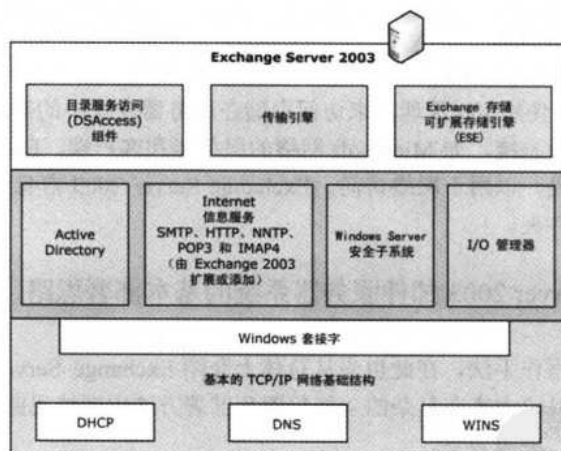


图 6-2 Exchange Server 2003 的网络组件

Exchange Server 2003 需要下列网络组件。

1) IP 和 TCP

Exchange Server 2003 需要 TCP/IP 来与网络中的其他计算机通信。Exchange Server 2003 不支持其他网络协议。

2) DNS

Exchange Server 2003 需要 DNS 来解析 TCP/IP 网络上的其他主机的 IP 地址、找到 Active Directory 域中的域控制器和全局编录服务器，以及找到其他邮件组织中的电子邮件服务器。

316 网管员必读——网络应用（第2版）

3) DHCP 和 WINS

Exchange Server 2003 不需要动态主机配置协议（DHCP）即可工作，但是，TCP/IP 网络中的一些网络客户端可能需要此项服务。DHCP 用于自动为网络上的计算机分配 IP 地址。另一方面，Windows 客户端使用 Windows Internet 名称服务（WINS）来执行 NetBIOS 名称解析。如果网络环境中包含不将广播分组转发到网段的路由器，则需要使用 WINS 来解析网络上其他计算机的 IP 地址。Exchange Server 2003 需要 WINS。

4) Windows 套接字

Exchange Server 2003 使用 Windows 套接字为连接到服务器所提供服务的网络客户端提供连接点。Windows 套接字是主机 IP 地址与端口号（用于标识服务器所提供的服务）的组合。

5) Active Directory

Active Directory 为 Exchange Server 2003 提供目录服务。

6) Internet 信息服务（IIS）

Exchange Server 2003 需要 IIS 来提供 Internet 协议支持。所有 Internet 协议服务（如 HTTP、SMTP 或 IMAP）均运行在 Exchange Server 服务器上的 IIS 处理环境中。

7) 安全子系统

Exchange Server 2003 使用 Windows Server 2003 的安全子系统来验证 Exchange 组织中的用户的身份。安全子系统确保了只有已经授权的用户才能够访问邮箱或向指定的收件人发送电子邮件。

8) Windows I/O 管理器

运行 Exchange Server 的服务器上的 I/O 管理器管理数据在服务器硬盘之间的传输。Exchange Server 2003 使用 I/O 管理器来访问存储在服务器硬盘中的事务日志和数据库。I/O 管理器还控制网络文件系统，如 Microsoft 网络的服务器和客户端。Exchange Server 2003 共享几个文件系统文件夹，以用于网络访问。Exchange Server 2003 自身使用 Microsoft 网络文件系统来访问这些文件夹。

6.1.4 Exchange Server 2003 邮件服务器系统的基本部署思路

遵循本书一贯的写作手法，在此也先从总体上介绍 Exchange Server 2003 邮件服务器系统的基本部署思路，以便大家在复杂的功能配置和部署方法中理清思路。这对于这样一款大型的邮件服务器来说，更为必要。

Exchange Server 2003 邮件服务器系统中涉及的功能和配置非常多，在此仅以最常见的企业邮局系统的应用需求为主线进行介绍。基本部署思路如下。

1) Exchange Server 2003 邮件服务器系统程序的安装

这看似是程序安装，但是它同样不可忽视，因为它的安装并非一般的 Windows 程序那么简单，需要符合许多复杂的安装条件。只要在所有条件满足后，才能得到顺利安装。

在这里的安装中，需重点注意系统环境的测试，它是程序安装的前期准备。

具体安装准备与程序安装方法与步骤参见本章 6.2 节的内容。

2) 邮件服务器系统的全局设置

因为 Exchange Server 2003 邮件服务器系统不仅是一个支持多邮件域、多邮件服务器的

大型邮件服务器系统，而且它还可以通过路由方式与网络中其他的 Exchange Server 2003 邮件服务器系统进行互联。当然本章因篇幅的因素不详细介绍服务器系统的路由配置。

在 Exchange Server 2003 邮件服务器系统的全局设置中主要介绍与邮件格式和邮件传递有关的属性选项设置方法。

具体设置方法与步骤参见本章 6.3 节的内容。

3) 邮件服务器设置

这是针对具体的邮件服务器进行的通用属性设置，主要介绍邮件服务器的区域设置、邮箱管理、安全、策略和目录访问等。

具体邮件服务器设置方法与步骤参见本章 6.4 节的内容。

4) 公用文件夹存储和邮箱存储的创建与设置

公用文件夹存储是服务器公用文件夹的存储设备。Exchange 支持多个公用文件夹存储，每个公用文件夹存储都包含在一个存储组中。每个公用文件夹存储又与一个公用文件夹树（也称为公用文件夹层次结构）关联。该树必须在创建公用文件夹存储之前即存在。只能将一个公用文件夹存储从与一棵树关联更改为与另一棵树关联。一般情况下无须另外添加公用文件夹存储，直接采用系统安装时默认创建的公用文件夹存储即可。只是在比较大型的邮件域中，在需要对公用文件夹进行分类时才需要另外创建，所以创建公用文件夹存储为可选工作。

邮箱存储是服务器邮箱的存储设备，也就是用户、组等其他对象的邮箱存储地。Exchange 也支持每个服务器中包含多个邮箱存储（可按一定规则分类），每个邮箱存储都包含在一个存储组中。在需要多个邮箱存储时就需要另外创建，因为系统默认也只创建一个邮箱存储。

具体创建与设置方法参见本章 6.5 节的内容。

5) 用户和组对象邮箱的创建与设置

邮件服务器系统中不能没有用户和组对象的账户，否则也就失去了服务器存在的意义。在 Exchange Server 2003 邮件服务器系统中，用户和组对象的邮箱账户是在“Active Directory 用户和计算机”管理单元中创建与设置的。

具体创建与设置方法参见本章后面的 6.6 节的内容。

6) 策略和的创建与设置

在 Exchange Server 2003 邮件服务器系统中支持多种不同类型的策略，其中包括收件人策略和系统策略两大类。收件人策略是应用于已启用邮件的 Exchange 对象（至少具有一个电子邮件地址的任何对象）以生成电子邮件地址的策略。系统策略是创建并应用于服务器、邮箱存储或公用存储的策略。

Exchange Server 2003 有两种收件人策略：电子邮件地址收件人策略和邮箱收件人策略；而“系统策略”又包括：服务器策略、公用存储策略和邮箱存储策略 3 种类型。

具体创建与设置方法参见本章 6.7 节的内容。

7) SMTP 协议设置

在 Exchange Server 2003 中所支持的邮件协议比较齐全，在此仅介绍最常使用、使用最多的 SMTP 协议设置。它们关系到邮件服务器系统能否正常进行邮件转发。

具体设置方法与步骤参见本章 6.8 节的内容。

8) 创建地址列表（可选）

地址列表一般也无须另外创建，直接采用邮件服务器系统程序安装时创建的地址列表即

318 网管员必读——网络应用（第2版）

可。只是在大型的邮件域中，需要对用户地址进行分类时才需要另外创建，所以也为可选项。

具体创建方法与步骤参见本章 6.9 节的内容。

9) 客户端邮件系统的配置

在此仅以最常见的 Outlook Express(Outlook 程序的配置方法一样)和 Outlook Web Access 为例进行介绍。

具体配置方法参见本章 6.10 节的内容。

10) 邮件服务器系统的管理

邮件服务器系统的管理主要包括：收件人管理（如启用、禁用 Exchange 功能）、队列查看与管理、查看电子邮件、删除邮件、冻结和解冻结邮件、监视邮件服务器性能、查看事件日志和事件查看器、监视邮件流等。

具体管理方法参见本章 6.11 节的内容。

6.2 Exchange Server 2003 的部署与安装

Exchange 的部署与安装一直以来都是相当复杂的，条件也很苛刻，而且需要花费相当长的时间。新版本的 Exchange Server 2003 也在安装条件上更加苛刻，但对以前版本进行了优化，安装时间有了明显缩短。但连同安装 SP2 补丁一起，也起码要一个小时以上。当然，最困难的不是时间问题，而是其中的安装条件验证，也就是系统安装前的部署，这是进一步安装的前提。因为这里的安装相对普通的 Windows 程序安装要复杂许多，所以本节将比较详细地介绍整个安装过程。下面首先了解一下 Exchange Server 2003 在安装方面有哪些改进。

6.2.1 Exchange Server 2003 安装程序的改进

Exchange Server 2003 安装程序包括很多新的功能，这些功能可以使大家在组织中部署 Exchange Server 2003 的工作变得更容易。这些新功能包括以下几方面。

1) 在 Active Directory 连接器和 Exchange 中使用相同的架构文件

在 Exchange 2000 中，Active Directory 连接器（ADC）架构文件是 Exchange 2000 核心架构文件的子集。在 Exchange Server 2003 中，在 ADC 升级期间所导入的架构文件与核心 Exchange Server 2003 架构文件是相同的。因此，只需更新架构一次。

2) 安装程序不需要组织级别的完全控制权限

在 Exchange 2000 中，运行安装程序的用户账户必须具有组织级别的 Exchange 管理员（完全控制）权限。在 Exchange Server 2003 中，虽然域中的第一台服务器必须由具有组织级别的 Exchange 管理员（完全控制）权限的用户安装，但具有管理组级别的 Exchange 管理员（完全控制）权限的用户可以安装其他服务器。

3) 安装程序不再联系架构 Flexible Single Master Operations 角色

在 Exchange 2000 中，安装程序或更新程序在每次运行时都会与架构 Flexible Single Master Operations（FSMO）角色联系。在 Exchange Server 2003 中，安装程序则不会联系架构 FSMO 角色。

4) ChooseDC 开关

Exchange Server 2003 安装程序包括新增的 ChooseDC 开关。现在，可以输入 Windows 域控制器的完全限定域名（FQDN），以强制安装程序从指定的域控制器读取和写入所有数据（指定的域控制器必须驻留在安装 Exchange Server 2003 服务器的域中）。同时安装多台 Exchange Server 2003 服务器时，通过强制每台服务器与同一个 Active Directory 目录服务域控制器通信，可以确保复制延迟不会干扰安装程序并导致安装失败。

5) 仅指派一次组织级别的默认权限

现在，Exchange Server 2003 安装程序仅指派一次 Exchange 组织对象的默认权限（在第一次服务器安装或升级期间），在后续安装过程中不再重新指派权限。以前，Exchange 2000 安装程序在每个服务器安装期间都会重新指派 Exchange 组织的权限。此操作会覆盖对权限结构的任何自定义更改。例如，如果允许所有用户创建顶级公用文件夹，那么，将在每次安装或升级期间删除这些权限。

6) 移动、删除或重命名 Exchange 组时显示警告消息

Exchange Server 2003 安装程序确保 Exchange Domain Servers 组和 Exchange Enterprise Servers 组完好无损。如果管理员已经移动、删除或重命名这些组，安装程序会停止运行，并显示警告消息。

7) 访问邮箱的权限

Exchange Server 2003 安装程序会配置用户邮箱对象上的权限，以使任何一个在组织级别和管理组级别应用了标准 Exchange 安全角色的组成员都无法打开其他用户邮箱，标准 Exchange 安全角色包括 Exchange 管理员（完全控制）、Exchange 管理员、Exchange 管理员（仅查看）角色。

8) 域用户拒绝本地登录权利

无论是安装还是升级到 Exchange Server 2003，Exchange 安装程序都不允许 Domain Users 组的成员以本地方式登录到 Exchange 服务器。

9) 默认情况下设置的邮件大小限制

如果还没有设置“发送邮件大小”和“接收邮件大小”的值，Exchange 安装程序会将这些值限制为不超过 10 240KB（10MB）。从 Exchange 2000 升级到 Exchange Server 2003 时，如果已经设置“发送邮件大小”和“接收邮件大小”，则会保留该值。

10) 默认情况下设置的公用文件夹的项目大小

如果还没有设置公用文件夹的项目大小，Exchange 安装程序会将该值限制为不超过 10240KB（10MB）。从 Exchange 2000 升级到 Exchange Server 2003 时，如果已经设置公用文件夹的项目大小，则会保留该值。

11) 自动完成 IIS 6.0 的配置

在 Windows Server 2003 中，IIS 6.0 引入了工作进程隔离模式，该模式为 Web 服务器提供了更高的可靠性和安全性。工作进程隔离模式确保与特定应用程序关联的所有身份验证、授权、Web 应用程序进程和 Internet 服务器应用程序编程接口（ISAPI）扩展都与所有其他应用程序隔离。在运行 Windows Server 2003 的计算机上安装 Exchange Server 2003 时，Exchange 安装程序将把 IIS 6.0 自动设置为工作进程隔离模式。

在默认情况下，在 Windows Server 2003 安装期间不会启用 ISAPI 扩展。但是，因为某些 Exchange 功能（如 Outlook Web Access、WebDAV 和 Exchange Web 表单）依赖于某些 ISAPI

320 网管员必读——网络应用（第2版）

扩展，所以，Exchange 安装程序会自动启用这些必需的扩展。

12) 在从 Windows 2000 升级到 Windows Server 2003 时自动完成 IIS 6.0 配置

如果将 Exchange Server 2003 安装在 Windows 2000 Server 上，并且随后升级到 Windows Server 2003，那么，Exchange 系统助理会将 IIS 6.0 自动设置为工作进程隔离模式。事件查看器将包含一个事件，指示已发生了此模式更改。升级之后，用户可能发现其他应用程序的一些 ISAPI 扩展在工作进程隔离模式下工作不正常。尽管可以将 IIS 6.0 模式设置为“IIS 5.0 隔离模式”以确保与 ISAPI 扩展的兼容，但建议用户应当继续在工作进程隔离模式下运行 IIS 6.0。在 IIS 5.0 隔离模式下，Exchange Server 2003 功能（如 Outlook Web Access、WebDAV 和 Web 表单）无法工作。

6.2.2 Exchange Server 2003 安装前的准备

在本节前面就介绍到，Exchange Server 2003 的安装条件非常之多，而且非常复杂，如果在安装前一一核对这些安装条件是否满足，则很可能造成程序无安装。本节先来介绍所需满足的各种条件，这些条件的具体配置方法将在 6.3 节介绍。

1. Exchange Server 2003 的全系统要求

安装 Exchange Server 2003 之前，请确保网络和服务器满足以下全系统要求。

- 域控制器正在运行 Windows 2000 Server Service Pack 3 (SP3) 或 Windows Server 2003。
- 全局编录服务器正在运行 Windows 2000 SP3 或 Windows Server 2003。建议每个计划安装 Exchange Server 2003 的域中都要有全局编录服务器。
- 在 Windows 站点中，已正确配置 DNS 和 WINS 服务。
- 要安装 Exchange Server 2003 的邮件服务器正在运行 Windows 2000 SP3 或 Windows Server 2003 Active Directory。

2. Exchange Server 2003 的服务器特定要求

安装 Exchange Server 2003 之前，请确保服务器满足这一节中描述的要求。如果服务器不满足所有要求，Exchange Server 2003 安装程序将停止安装。

下面是 Exchange Server 2003 服务器的最低硬件要求及推荐的硬件要求。

- Intel Pentium 133 MHz 或更快的处理器。

事实上这样的配置肯定是不行的，否则即使安装了也很难有效工作，建议至少采用 Intel Pentium 4 2.0GHz 处理器。

- 建议至少使用 256 MB 内存，最低支持 128MB。

同样，这也只是基本配置，没有多大实际意义，建议最少是 512MB，通常是需要 1GB 以上。

- 安装 Exchange 的驱动器上应具备 500 MB 的可用磁盘空间。

这是安装基本的 Exchange Server 2003 系统的磁盘空间需求，如果安装了 SP2，则至少是 1GB。因为邮件服务器上通常也会在本机保存用户邮件，所以在邮件服务器本机邮件存储目录中至少应该有 10GB 以上的空间预留。

- 系统驱动器上应具备 500 MB 的可用磁盘空间。

- CD-ROM 驱动器。
- SVGA 或分辨率更高的显示器。



其实以上条件仅作为参考，是没有多少实际意义的。因为事实已证明，如果仅满足以上硬件条件是远远不能满足的。笔者服务器处理器为 P4 2.4C、1GB 内存、ATA/133 的磁盘，安装系统都花了一个多小时，而且安装重启，或关机 Windows Server 2003 域控制器至少要 10 分钟。试想一下，如果仅是 133MHz 的处理器、128MB 内存的情况下，该是多么糟糕。

3. 文件格式要求

要安装 Exchange Server 2003，磁盘分区格式必须采用 NTFS 文件系统，而不能采用文件分配表（FAT）。该要求适用于下列分区。

- 系统分区。
- 存储 Exchange 二进制数据的分区。
- 包含事务日志文件的分区。
- 包含数据库文件的分区。
- 包含其他 Exchange 文件的分区。

4. 操作系统要求

下列操作系统支持 Exchange Server 2003。

- Windows 2000 SP3 或更高版本。
- Windows Server 2003。

5. 系统服务要求

Exchange Server 2003 安装程序要求在服务器上安装，并启用下列组件和服务。

- .NET Framework。
- ASP.NET。
- Internet 信息服务（IIS）。
- World Wide Web Publishing 服务。
- 简单邮件传输协议（SMTP）服务。
- 网络新闻传输协议（NNTP）服务。

如果在运行 Windows 2000 的服务器上安装 Exchange Server 2003，则 Exchange 安装程序会自动安装并启用 Microsoft .NET Framework 和 ASP.NET。在运行 Exchange Server 2003 安装向导之前，必须手动安装 World Wide Web Publishing 服务、SMTP 服务和 NNTP 服务。这些都可以在“添加或删除程序”工具中进行。而且，如果在原始 Windows Server 2003 目录林或域中安装 Exchange Server 2003，默认情况下不会启用这些服务。在运行 Exchange Server 2003 安装向导之前，必须手动启用这些服务。



在新服务器上安装 Exchange 时，将只启用必需的服务。例如，默认情况下在所有 Exchange Server 2003 服务器上禁用邮局协议版本 3（POP3）、Internet 邮件访问协议版本 4（IMAP4）和 NNTP 服务。应当只启用对于执行 Exchange Server 2003 任务来说必不可少的服务。一定不能安装 POP3、IMAP4 邮件服务器系统。

6.2.3 服务器安装前的系统准备

在这一节中将介绍整个 Exchange Server 2003 第一台服务器安装过程中的系统准备步骤，其中包括 Exchange Server 2003 邮件服务器部署 8 个步骤中的前 3 个步骤，它们分别是：系统平台验证、服务启动和支持工具。具体步骤如下。

(1) 将 Exchange Server 2003 CD 插入 CD-ROM 驱动器中，如果程序是放在磁盘中，可直接双击运行其根目录下的 Setup.exe 文件，均可打开如图 6-3 所示“欢迎使用 Exchange Server 2003 安装程序”界面。



图 6-3 “欢迎使用 Exchange Server 2003 安装程序”界面

(2) 单击右栏下部的【Exchange 部署工具】链接，打开如图 6-4 所示界面。在这里可以选择几种安装部署方式，如可以是部署第一台 Exchange Server 2003 邮件服务器，也可以进行在其他服务器上安装 Exchange Server 2003，还可以在已安装了 Exchange Server 2003 系统的服务器上执行安装后的其他操作和安装 Exchange Server 2003 系统管理工具。



图 6-4 “欢迎使用 Exchange Server 部署工具”界面

(3) 单击【部署第一台 Exchange 2003 服务器】链接，打开如图 6-5 所示界面，进行第一台邮件服务器的安装与部署。在这里又提供了几种服务器安装选择，具体选择哪种要根据当前系统环境而定。本例中是在 Windows Server 2003 系统中安装第一台 Exchange Server 2003 服务器，而不是从以前版本的 Exchange 2000 服务器中升级，也不是想与以前的 Exchange 5.5、

Exchange 2000 系统共享用户数据库，所以在此要单击【安装全新的 Exchange 2003】链接。

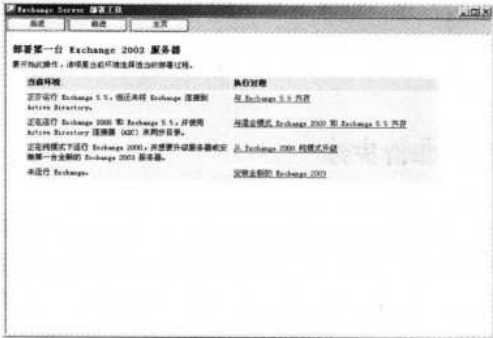


图 6-5 “部署第一台 Exchange 2003 服务器”界面

(4) 单击【安装全新的 Exchange 2003】链接后，打开如图 6-6 所示界面。在这里列出了全新安装中的 8 个必需执行的步骤。具体如下。



图 6-6 部署第一台 Exchange 2003 服务器的 8 个步骤界面

- 验证网络服务器操作系统满足指定的要求。要求是 Windows 2000 Server SP3 或更高版本、Windows 2000 Advanced Server SP3，或者 Windows Server 2003 系统。
- 安装并启用必需的 Windows 服务。这些服务包括 NNTP、SMTP，当然必须安装 IIS 组件。如果是在 Windows Server 2003 系统中安装，则还要安装并启用 ASP.NET。
- 确保网络服务器系统加安装了系统支持工具，因为在安装过程中要用到其中的 DCdiag 和 Netdiag 两个工具。
- 运行 DCdiag 工具。这是安装前的网络连接和 DNS 解析测试。
- 运行 Netdiag 工具。这是安装前的网络连接测试。
- 运行 ForestPrep。这个工具是 Exchange Server 2003 程序自带的，是用于安装前的 Active Directory 架构扩展，也就是林的准备。
- 运行 DomainPrep。这个工具也是 Exchange Server 2003 程序自带的，是用于安装前

的域准备。

- 运行 Exchange 安装程序。这才是真正的 Exchange Server 2003 程序安装。

在以上 8 个步骤中,前面 7 个都属于准备过程,只有最后一个步骤才是真正的程序安装。都将后面各节具体介绍。

6.2.4 程序安装前的 7 个准备步骤

上节介绍了在整个 Exchange Server 2003 邮件服务器程序正式安装前需要进行 7 个必须进行的准备步骤。只有在完全确认以上步骤都完成，并且符合要求了后才可以进行正式的程序安装。这也就是程序安装的基本条件。下面分别对如图 6-6 所示界面中列出的 8 个步骤中的前 7 个步骤进行一一介绍。

1. 网络服务器系统的验证

在如图 6-6 所示的第 1 个步骤中,要求检查当前系统是否满足 Exchange Server 2003 服务器安装的系统要求,具体系统要求如下。

- 域控制器正在运行 Windows 2000 Server Service Pack 3 (SP3) 或 Windows Server 2003。
- 全局编录服务器正在运行 Windows 2000 SP3 或 Windows Server 2003。建议每个计划安装 Exchange Server 2003 的域中都要有全局编录服务器。
- 在 Windows 站点中, 已正确配置 DNS 和 WINS 服务。
- 服务器正在运行 Windows 2000 SP3 或 Windows Server 2003 Active Directory。

2. 检查所安装的服务

在如图 6-6 所示的第 2 步是检查在当前系统中是否安装,并启用了 ASP.net、NNTP、SMTP 和万维网服务等服务。如果在运行 Windows 2000 的服务器上安装 Exchange Server 2003,则 Exchange 安装程序会自动安装并启用 Microsoft .NET Framework 和 ASP.NET。在运行 Exchange Server 2003 安装向导之前,必须手动安装 World Wide Web Publishing 服务、SMTP 服务和 NNTP 服务。

如果在原始 Windows Server 2003 目录林或域中安装 Exchange Server 2003，在默认情况下不会启用这些服务。在运行 Exchange Server 2003 安装向导之前，必须手动启用这些服务。这些服务的安装很简单，在此以 Windows Server 2003 系统为例进行介绍。

(1) 在“控制面板”中选择“添加或删除程序”工具, 打开如图 6-7 所示界面。



图 6-7 “添加或删除程序”界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 单击【添加/删除 Windows 组件】按钮，在打开的对话框中选择“应用程序服务器”选项，如图 6-8 所示。

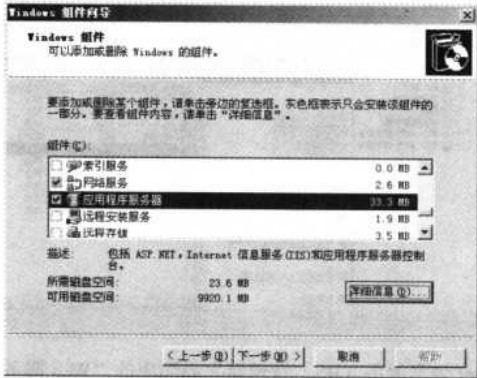


图 6-8 “Windows 组件”界面

(3) 单击【详细信息】按钮，打开如图 6-9 所示界面，在其中选择“ASP.NET”和“Internet 信息服务”两个选项。

(4) 选择“Internet 信息服务”选项，再单击【详细信息】按钮，打开如图 6-10 所示的对话框。在其中要同时选择“NNTP Service”、“SMTP Service”和“万维网服务”3 个选项，不过此时系统会自动选择“公用文件”选项。

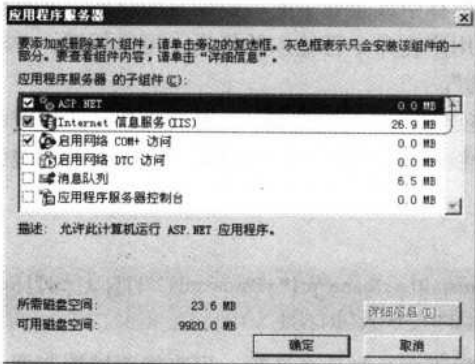


图 6-9 “应用程序服务器”对话框

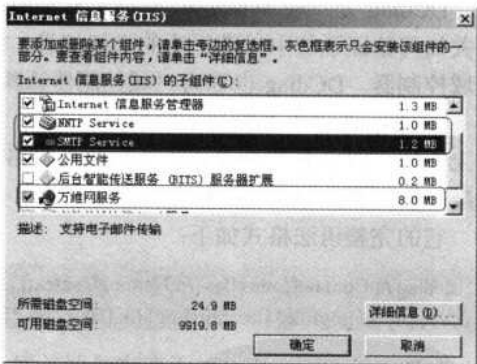


图 6-10 “Internet 信息服务 (IIS)”对话框

(5) 依次单击【确定】按钮返回，到图 6-8 所示界面时单击【下一步】按钮，系统会自动安装所配置的 Windows 组件的。

(6) 启动 ASP.NET 服务。执行【开始】→【管理工具】→【Internet 信息服务 (IIS) 管理器】菜单操作，在打开的主界面左边控制台树中选择“Web 服务扩展”容器选项，在右边详细信息列表中选择“ASP.NET v1.1.4322”选项，然后单击中间的【允许】按钮。最好用同样的方法确保其中的“Active Server Pages”选项也为“允许”状态，如图 6-11 所示。

3. 安装系统支持工具

安装 Windows 支持工具。在 Windows Server 2003 系统中找到“Support\Tools”路径，双

击执行其中的 Suptools.msi 文件，打开一个安装向导安装所需的支持工具程序即可。安装支持工具后才可使用 DCdiag 和 Netdiag 测试工具。



图 6-11 “Internet 信息服务 (IIS) 管理器”界面中的“Web 服务扩展”选项窗口

4. 用 DCdiag 工具测试网络连接和 DNS 解析

在如图 6-4 所示的第 4 步就是利用第 3 步所安装的 Windows 系统工具 Dcdiag 来测试当前服务器系统的网络连接和 DNS 解析是否正常。

执行【开始】→【所有程序】→【附件】→【命令提示符】菜单操作，进入命令提示符状态。首先执行 DCdiag.exe 命令测试域控制器架构是否符合 Exchange Server 2003 邮件服务器安装条件和当前账户是否具备相应权限。

DCdiag 是一种 Windows 支持工具，用于分析林中或企业中的域控制器的状态，并提供有关如何验证系统中异常行为的详细信息。根据用户在命令行输入的指令，可以标识，并测试域控制器。DCdiag 也称为“域控制器诊断工具”。

DCdiag 在以下系统功能区域执行测试：网络连接性、复制结构、拓扑完整性，并检查命名上下文（NC）标题安全描述符；检查网络登录权利；定位程序获取域控制器；站点间健康状况；检查服务器角色；信任验证。

它的完整语法格式如下：

```
dcdiag /s:DomainController [/n:NamingContext] [/u:Domain\UserName /p:{* | Password | ""}] [{/a | /e}] [{/q | /v}] [/i] [/f:LogFile] [/ferr:ErrLog] [/c [/skip:Test]] [/test:Test] [/fix] [{/h | /?}]
```

/s:DomainController 对于在成员服务器上运行该命令时是必选项，用来指明域控制器。但当在域控制器上执行该命令时，将忽略该参数选项，所以可以不用该参数。在此处测试时不必详细输入以上这么多参数，只需输入/f:LogFile 参数即可，把测试结果保存在一个日志文件中。也可同时加上/ferr:ErrLog 参数，把输入的错误事件写入到错误日志文件中，以便查阅。如果不加上这两个参数，则测试会直接在屏幕中滚动，不便于工作查阅。

此处仅加上/f:LogFile 参数，其他参数均可不用。只需在命令提示符下输入：DCdiag /f:日志文件名（如 dcdiag /f:dcdiaglog）即可。回车后很快完成测试，再到当前账户的配置文件目录下找到上述 dcdiag 日志记录文件，用记事本程序打开，则可查看所有测试项目的通过情况，如图 6-12 所示。主要查看输出中的“Doing Primary Tests”（主测试）项下面的诸多测试项，如果此处的测试项通过（Passed）了，如图 6-12 所示，则一般来说证明该网络中的域控制器和当前账户符合安装条件。

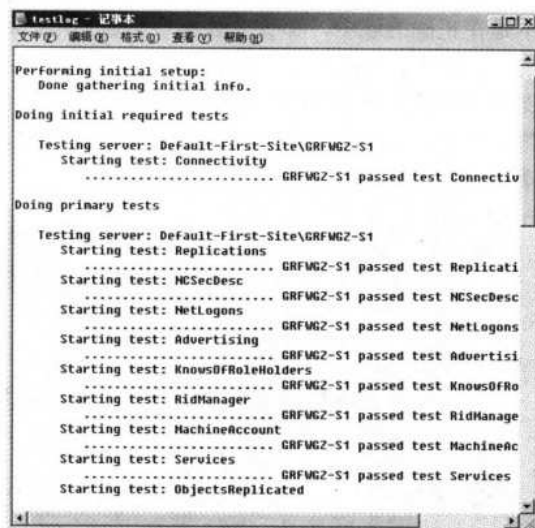


图 6-12 DCdiag.exe 测试日志文件

5. 用 Netdiag 工具进一步测试网络连接

上述 DCdiag 测试通过后，立即运行 Netdiag.exe 工具命令进行网络测试。Netdiag.exe 也是 Windows 支持工具，与 DCdiag.exe 类似，不过它是用来检查端对端网络，以及已分配的服务功能的。它的完整语法格式如下：

```
netdiag [/q] [/v] [/l] [/debug] [/d: DomainName] [/fix] [/DcAccountEnum] [/test: TestName]
[/skip:TestName] [/?]
```

如果加有 /q 则以快速方式显示测试输出，仅显示错误项目。其他具体参数说明参见系统帮助说明。

在此可直接在命令提示符下输入 Netdiag 命令，不带任何参数。虽然没有配置输出的日志文件，但系统会自动把测试结果以日志文件形式输出，日志文件名为 Netdiag.log，运行界面如图 6-13 所示。同样可在当前用户账户配置文件目录下找到这个日志文件，同样可以用记事本程序打开。如果测试成功，则会在测试界面和日志文件最后显示“The command completed successfully”。检查日志中的失败项目，如果认为确实没必要的，如默认网关、WAN 配置等，则可忽略。如果不是可忽略的，则要依次进行手动修复。

6. 利用 ForestPrep 工具进行 Active Directory 架构扩展

Exchange Server 2003 程序中的 ForestPrep 工具命令可用于扩展 Active Directory 架构（其实可以从这个工具名称得知，它是用于域网络林的准备，因为其中的“Forest”就是“林”的意思），使其包含 Exchange 特有的类和属性。ForestPrep 还会在 Active Directory 中为 Exchange Server 2003 组织创建容器对象。Exchange Server 2003 提供的架构扩展是 Exchange 2000 提供的架构扩展的超集。即使在原有 Exchange 2000 服务器中已经运行了 Exchange 2000 ForestPrep，仍然必须再次运行 Exchange Server 2003 ForestPrep。

运行 ForestPrep 程序必须在架构主机所在的域中进行。在默认情况下，架构主机运行在目录林中第一个安装的 Windows 域控制器上。Exchange 安装程序会验证是否在正确的域中

328 网管员必读——网络应用（第2版）

运行 ForestPrep。如果不是在正确的域中，那么安装程序会通知用户哪个域包含架构主机。用来运行 ForestPrep 的账户必须是 Enterprise Administrator 和 Schema Administrator 组的成员。运行 ForestPrep 时，需要你指定对组织对象拥有 Exchange 管理员（完全控制）权限的账户或组。此账户或组有权在整个目录林内安装和管理 Exchange Server 2003。安装第一台服务器之后，此账户或组还有权委派其他 Exchange 管理员（完全控制）权限。具体步骤如下。

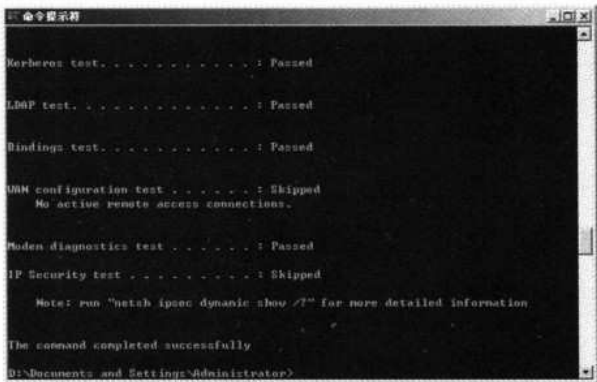


图 6-13 执行 Netdiag.exe 命令的运行界面

(1) 在如图 6-6 所示界面中的第 6 步中，可在“可指定程序安装路径”文本框中输入 Exchange Server 2003 系统源程序的安装路径（程序根目录即可）。然后直接单击【立即运行 ForestPrep】链接，打开如图 6-14 所示的安装向导对话框。



图 6-14 “欢迎使用 Microsoft Exchange 安装向导”对话框

(2) 单击【下一步】按钮，打开如图 6-15 所示的对话框。在这里选择“我同意”单选项。

(3) 单击【下一步】按钮，打开如图 6-16 所示的对话框。在这里要正确输入有效的 Exchange Server 2003 产品的标识号，也就是通常所说的产品密钥。这在产品包装上有说明。

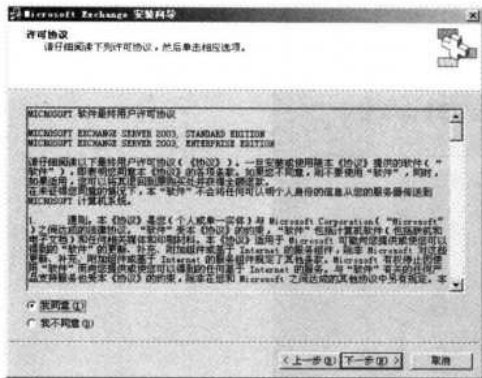


图 6-15 “许可协议”对话框

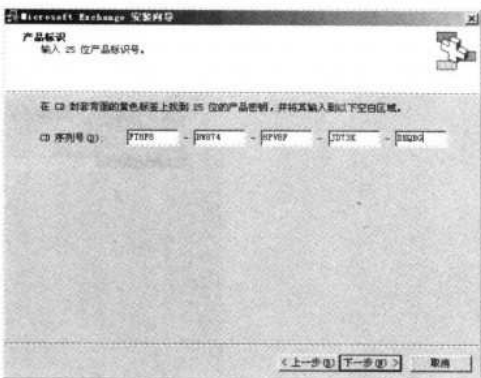


图 6-16 “产品标识”对话框

(4) 单击【下一步】按钮，如果上节所介绍的各主要项测试成功的话，很快会打开如图 6-17 所示的对话框。否则可能会耗费很长的时间，而最后还是不能显示完整的如图 6-17 所示的对话框，因为在对话框中“操作列”没有显示“ForestPrep”选项。强行选择也没用，同时会显示如图 6-18 所示的错误提示。

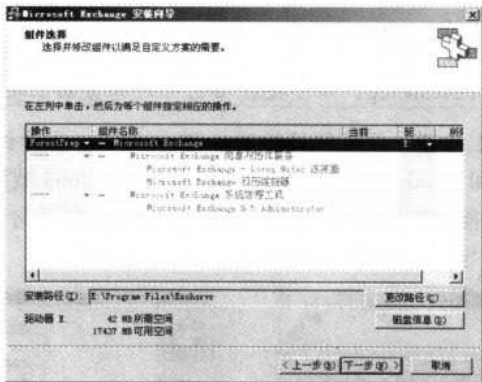


图 6-17 ForesPrep 程序安装过程中的“组件选择”对话框



图 6-18 无法进行 ForestPrep 安装的错误提示

(5) 单击如图 6-17 所示的对话框中的【下一步】按钮，打开如图 6-19 所示的对话框。在这里要配置一个赋予完全控制权限的用户账户。这个账户可以在邮件服务器安装完成后把一部分任务委派给其他用户或组账户。在此，基本上选择企业域管理员账户担当具有完全控制权限的账户，当然也可以是其他普通账户。

330 网管员必读——网络应用（第2版）

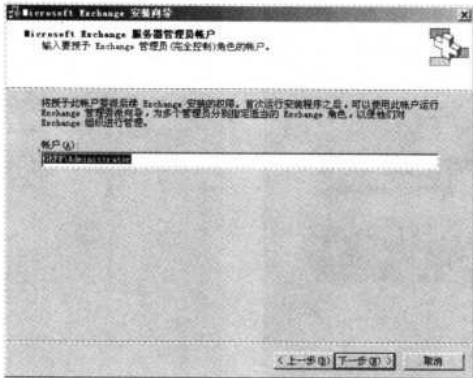


图 6-19 “Microsoft Exchange 服务器管理员账户”对话框



注意

向安全组委派 Exchange 角色时，建议用户使用全局安全组或通用安全组，而不要使用域本地安全组。尽管域本地安全组可以工作，但它们的作用域被限制在它们自己的域范围内。在很多情形中，Exchange 安装程序需要在安装期间向其他域进行身份验证。在这种情况下，Exchange 安装可能由于缺乏对外部域的权限而失败。

另外，为了减少复制时间，建议用户在根域内的域控制器上运行 Exchange Server 2003 ForestPrep，而不要在当前邮件服务器上运行。

(6) 单击【下一步】按钮，系统便开始进行 ForestPrep 程序组件安装，安装进程如图 6-20 所示。根据网络拓扑和 Windows 2000 或 Windows Server 2003 域控制器的速度，ForestPrep 可能需要经过较长时间才能执行完毕。完成后显示如图 6-21 所示向导完成对话框，单击【完成】按钮即可完成安装向导。

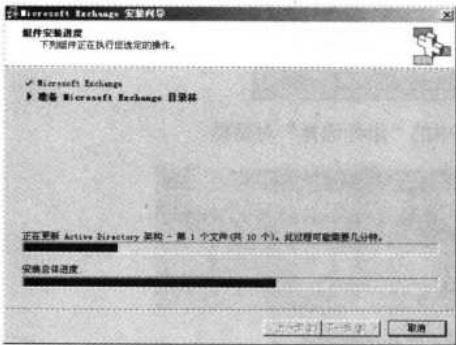


图 6-20 “组件安装进度”对话框



图 6-21 “正在完成 Microsoft Exchange 向导”对话框

7. 利用 DomainPrep 工具进行域准备

运行 ForestPrep 并且完成复制之后，必须运行 Exchange Server 2003 DomainPrep。DomainPrep 用于创建 Exchange 服务器在读取和修改用户属性时所必需的组和权限。Exchange Server 2003 版本的 DomainPrep 将在域中执行以下操作。

- 创建 Exchange Domain Servers 和 Exchange Enterprise Servers 组。

- 将全局 Exchange Domain Servers 组嵌套到 Exchange Enterprise Servers 本地组中。
- 创建“Exchange 系统对象”容器，该容器用于存放已启用邮件的公用文件夹。
- 在域的根位置设置 Exchange Enterprise Servers 组的权限，使收件人更新服务有正确的权限来处理收件人对象。
- 修改 Windows 用来为本地 Domain Administrator 组的成员设置权限的 AdminSdHolder 模板。
- 将本地 Exchange Domain Servers 组添加到 Pre-Windows 2000 Compatible Access 组中。
- 执行安装程序的安装前检查。

用来运行 DomainPrep 的账户必须是本地域中 Domain Administrators 组的成员和本地计算机管理员。必须在以下域中运行 DomainPrep。

- 根域。
- 将要包含 Exchange Server 2003 服务器的所有域。
- 将要包含启用了 Exchange Server 2003 邮箱的对象（如用户和组）的所有域，即使这些域中不会安装 Exchange 服务器。
- 将要负责管理 Exchange Server 2003 组织的 Exchange Server 2003 用户和组所在的所有域。



注意 运行 DomainPrep 时不需要任何 Exchange 权限。只有本地域中的 Domain Administrator 权限是必需的。

(1) 在如图 6-6 所示界面第 7 步单击【立即运行 DomainPrep】链接项，同样会打开如图 6-14 所示安装向导。按前面介绍的 ForestPrep 安装步骤，一直进行到出现如图 6-16 所示的对话框。

(2) 单击【下一步】按钮，出现的是如图 6-22 所示的对话框。在“操作”列中显示的是“DomainPrep”选项。



图 6-22 DomainPrep 程序安装过程中的“组件选择”对话框

(3) 单击【下一步】按钮，DomianPrep 程序组件即自动安装，安装进程如图 6-23 所

示。安装完成后同样会出现如图 6-21 所示的向导完成对话框。单击【完成】按钮即可完成安装向导。

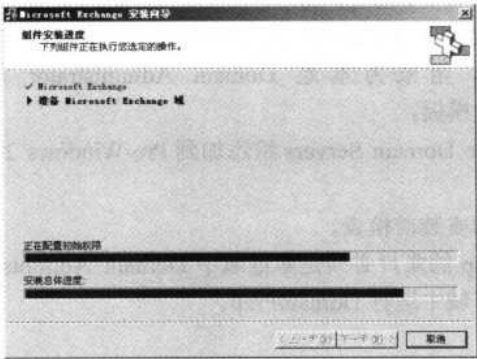


图 6-23 “组件安装程度”对话框

6.2.5 Exchange 程序的正式安装

这就是如图 6-6 所示的最后一步——第 8 步。要在目录林中安装第一台 Exchange Server 2003 服务器，必须使用在组织级别具有 Exchange 管理员（完全控制）权限，并且是计算机本地管理员的账户。具体来说，可以使用在运行 ForestPrep 时指定的账户或用户指定的组中的账户（参见图 6-19）。具体步骤如下。

（1）在如图 6-6 所示界面第 8 步单击【立即运行安装程序】链接项，同样会打开如图 6-14 所示安装向导。按前面介绍的 ForestPrep 安装步骤，一直进行直到出现如图 6-16 所示的对话框。

（2）单击【下一步】按钮，打开如图 6-24 所示的对话框。在这里可以进行比较详细的安装选择。不仅可以选择安装类型，如典型安装、最小安装等。还可以对相应类型安装中的各组件进行选择安装。在对话框下面将显示所选安装方式下，所需的磁盘空间大小，对照当前系统中的磁盘空间。



图 6-24 Exchange 程序安装过程中的“组件选择”对话框

(3) 单击【下一步】按钮，打开如图 6-25 所示的对话框。在这里选择安装类型。如果全新安装，则选择“新建 Exchange 组织”单选项，如果是加入原有 Exchange 组织，或者升级 Exchange 5.5 组织，则选择“加入或升级现有的 Exchange 5.5 组织”单选项。在此以全新安装为例，选择“新建 Exchange 组织”单选项。

(4) 单击【下一步】按钮，打开如图 6-26 所示的对话框。在这里要为新建的 Exchange 组织配置一个组织名称，如公司名称。名称必须至少包含 1 个字符，但应少于 64 个字符。在新的 Exchange Server 2003 组织名称中可以使用以下字符：A 到 Z、a 到 z、0 到 9、空格、连字符或破折号。

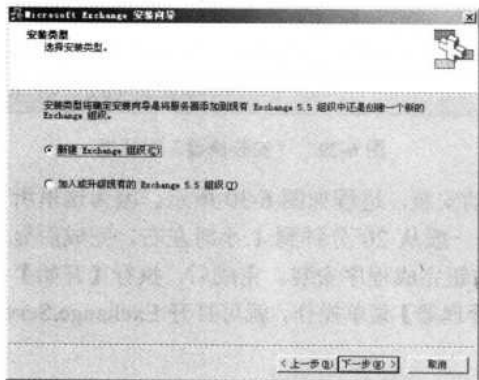


图 6-25 “安装类型”对话框

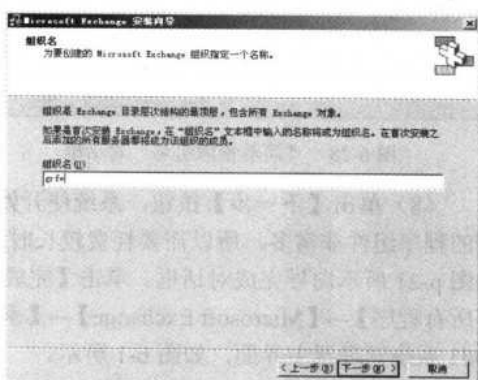


图 6-26 “组织名”对话框

(5) 单击【下一步】按钮，打开如图 6-27 所示的对话框。在这里选择是否同意授权协议，只能选择“我同意。我已阅读本产品的许可协议，并愿意遵守有关规定。”单选项。

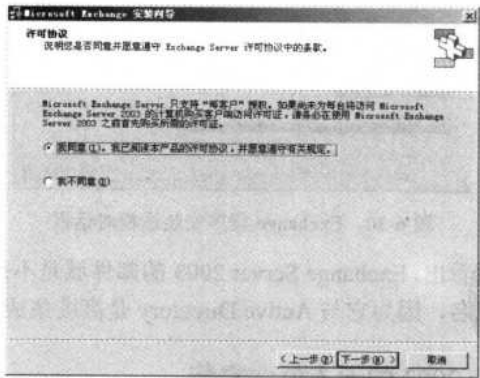


图 6-27 “许可协议”对话框

(6) 单击【下一步】按钮，打开如图 6-28 所示的对话框。如果在如图 6-26 所示的对话框中配置的组织名包括一些连接字符，则要在配置一个无连接符的简单组织名。当在如图 6-26 所示的对话框中配置的名称中不带连接符时，两个对话框中配置的名称也可以一样。

(7) 单击【下一步】按钮，打开如图 6-29 所示的对话框。这时显示了在如图 6-24 所示的对话框中的选择摘要，其中包括所选组件和对应所需的磁盘空间，方便用户进一步确认。

如果认为不妥，可通过单击【上一步】按钮重新选择所安装的组件。

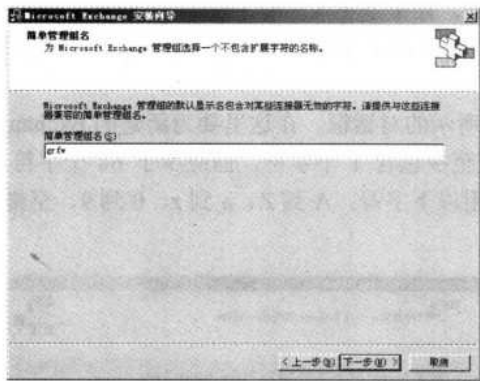


图 6-28 “简单管理组名”对话框

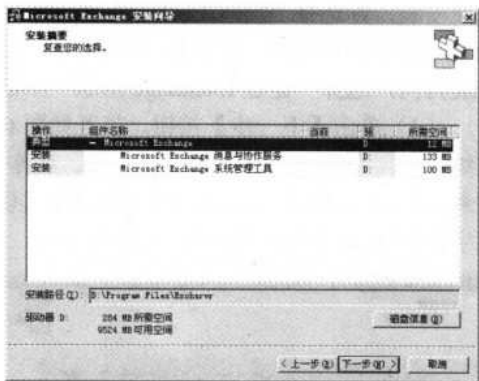


图 6-29 “安装摘要”对话框

(8) 单击【下一步】按钮，系统便开始自动安装，进程如图 6-30 所示。因为这里所安装的程序组件非常多，所以需要耗费较长时间。一般从 20 分钟到 1 小时左右。完成后显示如图 6-21 所示向导完成对话框。单击【完成】按钮完成程序安装。完成后，执行【开始】→【所有程序】→【Microsoft Exchange】→【系统管理器】菜单操作，就可打开 Exchange Server 2003 系统管理器主界面，如图 6-1 所示。

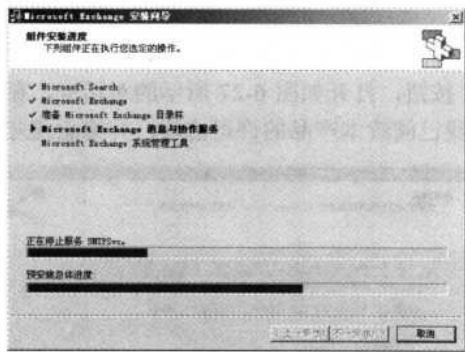


图 6-30 Exchange 程序安装进程对话框

从以上安装过程可以看出，Exchange Server 2003 的邮件域是不需要的，也不能重新配置，直接采用当前网络域的域名，因为它与 Active Directory 是高度集成的。

6.2.6 Exchange Server 2003 的无人值守安装

Exchange Server 2003 系统的无人参与安装方式与 Windows 系统的无人值守安装一样，微软的 Exchange Server 2003 也提供了无人值守安装方法。这主要应用于在具有密集邮件需要的大型组织中，部署多个 Exchange Server 2003 服务器，因为 Exchange Server 2003 邮件服务的部署是一件很耗时间和资源的工作。

要解决这个问题，可以在安装第一台 Exchange Server 2003 服务器之后采用无人值守模

式来安装随后的 Exchange 服务器，以便自动完成服务器的安装。Exchange Server 2003 服务器的无人值守安装程序将在没有任何提示或对话框的情况下运行并完成安装任务。此外，无人值守安装程序还会创建存储了示例配置信息的应答文件。然后，可以用该文件在多个服务器上安装 Exchange Server 2003。应答文件包含部署参数和示例配置，以便用户可以指定想要执行的安装类型。这些配置通常是在一台服务器上执行手动 Exchange Server 2003 安装时设置的。

1. 无人值守安装的条件

只能在满足本章前面的 Exchange Server 2003 系统安装各方面要求的服务器上运行无人值守安装程序。如果服务器不满足这些要求，则不要运行无人值守安装程序。

在以下步骤中可以运行无人值守安装程序。

- 在组织中安装第 2 台到第 n 台 Exchange Server 2003 服务器时。
- 安装 Exchange Server 2003 系统管理工具时。
- 运行 DomainPrep 时。

在以下步骤中不能运行无人值守安装程序。

- 在组织中安装第 1 台 Exchange Server 2003 服务器时。
- 在 Windows 群集中安装 Exchange Server 2003 时。
- 在混合模式环境中（例如，Exchange 5.5 和 Exchange Server 2003 组成的混合模式环境）安装 Exchange Server 2003 时。
- 执行任何维护任务（例如，添加或删除程序、重新安装 Exchange 或升级 Exchange 2000）时。

2. 创建应答文件

与 Windows 系统的无人值守（无人参与）安装一样，要实现无人值守安装必须先创建无人值守安装的应答文件。具体步骤如下。

（1）在满足安装 Exchange Server 2003 的先决条件的服务器上，将 Exchange CD 插入 CD-ROM 驱动器中。

（2）在命令提示符下键入 `X:\setup\i386\setup /createunattend M:\myanswerfile.ini`，其中 X 是 CD-ROM 驱动器盘符，M 是系统驱动器盘符，而 myanswerfile.ini 则代表想要在随后的安装中使用的应答文件。本例为 `G:\setup\i386\setup /createunattend E:\answerfile.ini`，首先打开的是如图 6-31 所示的对话框。



图 6-31 “欢迎使用 Microsoft Exchange 安装向导”对话框



警告

系统不会在命令行验证 Exchange Server 2003 Setup.exe 的命令行参数。如果 setup.exe /createunattend 开关出现任何拼写错误，将启动手动安装。在“摘要”页上单击【下一步】按钮之前，无法验证是在运行手动安装还是在运行无人值守模式安装。此时，在手动安装中，将开始进行 Exchange Server 2003 安装，并且无法取消。因此，在试图为无人值守安装 Exchange Server 2003 而创建和使用应答文件之前，应确保命令行开关拼写正确。

(3) 随后的步骤就如图 6-15 和图 6-16 所示。在“产品标识”页上，键入 25 位产品密钥。

(4) 在如图 6-16 所示的对话框中单击【下一步】按钮，打开如图 6-24 所示的对话框。在“组件选择”页上的“操作”列中，使用下拉箭头为每个组件指定合适的操作。



可以为下列任务创建应答文件：安装 Exchange Server 2003 服务器、仅安装 Exchange Server 2003 系统管理工具及运行 DomainPrep。

(5) 单击【下一步】按钮，打开类似如图 6-29 所示的对话框。在这里确认已正确设置 Exchange 安装选项。

(6) 单击【下一步】按钮，在打开的类似如图 6-21 所示“正在完成 Microsoft Exchange 向导”页上，单击【完成】按钮，完成应答文件的创建。

3. 使用应答文件运行无人值守安装程序

在想要以无人值守模式安装 Exchange Server 2003 的服务器上，将 Exchange CD 插入 CD-ROM 驱动器。在命令提示符处，键入 `X:\setup\i386\setup /unattendfile M:\answerfile.ini`，同样其中的 X 是 CD-ROM 驱动器，M 是系统驱动器，answerfile.ini 代表在前面创建的应答文件。然后，在不需要任何用户交互的情况下，Exchange Server 2003 将自动安装到服务器上。要验证 Exchange 安装是否成功。完成 Exchange Server 2003 部署之后，可以使用 Exchange Server 2003 安装程序日志和 Windows 事件查看器来验证安装是否成功。在验证部署之后，应在系统上使用最新的服务包和安全修补程序。

完成 Exchange 部署之后，请检查位于 Exchange 计算机 Windows 2000 Server，或者 Windows Server 2003 系统驱动器上的安装日志（Exchange Server Setup Progress.log）。安装程序日志包含有关安装的信息，并且用于验证 Exchange Server 2003 安装是否成功。

Exchange 安装程序还会将应用程序日志中的事件记录到运行 Windows 2000 Server 或 Windows Server 2003 的计算机上。

如果要通过访问事件查看器来验证，可执行【开始】→【管理工具】→【事件查看器】菜单操作，打开如图 6-32 所示控制台窗口。选择“应用程序日志”选项，可以查看“MSExchangeSetup”ID 项。

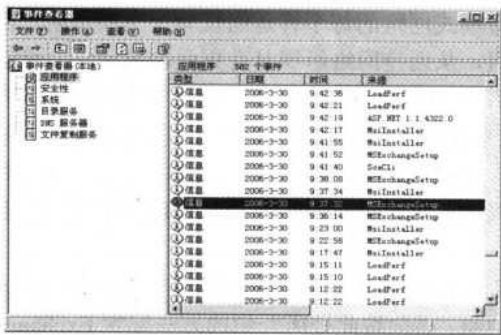


图 6-32 “事件查看器”窗口中的 MSEXCHANGESETUP 选项

6.3 Exchange Server 2003 服务器配置

Exchange Server 2003 邮件服务器安装好后，在正式使用之前也必须进行一些必要的属性配置。总体来说，Exchange Server 2003 邮件服务器的属性配置非常烦琐，也非常多。因为篇幅限制，不可能对所有节点属性配置一一介绍，所以在此仅选择一般企业邮件服务系统中必须进行典型属性配置进行介绍。

6.3.1 Exchange Server 2003 服务器根节点属性配置

(1) 在如图 6-1 所示系统管理器控制台左边控制树中选择根节点，也就是在安装 Exchange Server 2003 服务器程序时所配置的组织单位（本示例为 grfw），单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 6-33 所示的对话框。



图 6-33 Exchange Server 2003 服务器属性对话框“常规”选项卡

使用此对话框可以将 Exchange Server 2003 配置为是否在 Exchange 系统管理器的控制台树中显示路由组和管理组。还可以选择是以纯模式还是混合模式运行 Exchange Server 2003。Exchange Server 2003 允许在一个网络中集成 Exchange 5.x 和 Exchange Server 2003 服务器（混合模式），或在一个网络中仅包含 Exchange Server 2003 服务器（纯模式）。

338 网管员必读——网络应用（第2版）

在默认情况下，混合模式网络的每个管理组仅有一个路由组。而在纯模式网络中，可以单独配置管理组和路由组，从而使网络组织具有更强的灵活性。管理组是为方便管理而定义服务器和其他对象的逻辑组；路由组定义 Exchange 服务器的物理网络拓扑，这主要是针对大型的 Exchange 邮件系统来说的。管理组可以包含下列任意 Exchange 对象：服务器、策略、路由组和公用文件夹树。通过管理组，可以为管理组以及管理组中的对象委派特定的管理权限并指定系统策略。可以创建系统策略以便控制对管理组中的服务器、邮箱存储，以及公用文件夹存储的管理。

在 Exchange 2003 或 Exchange 2000 组织安装 Exchange 后，Exchange 系统管理器并不会自动显示管理组和路由组。必须按此处所介绍的方法配置 Exchange 组织显示管理组。在配置此设置后，可以查看“管理组”容器并为组织创建其他管理组。



如果在 Exchange 5.5 站点中安装 Exchange 2000（或更高版本），在默认情况下 Exchange 将启用管理组和路由组，每个 Exchange 5.5 站点都以管理组的形式出现。

“路由组”是用于控制邮件流和公用文件夹引用的服务器的逻辑集合。在路由组中，所有服务器彼此之间都直接通信并传输邮件。在路由组中，所有服务器彼此之间都直接通信并传输邮件，具体如下。

- Exchange 组织中的用户使用邮件客户端向另一个用户发送邮件。
- 发件人的客户端使用 SMTP 将该邮件提交到驻留客户端邮箱的 Exchange 服务器上的 SMTP 虚拟服务器。
- Exchange 服务器查找邮件的收件人，以确定收件人的邮箱驻留在哪一台服务器上。
- 或者是发生下面的两种情况之一。
 - ◇ 如果收件人的邮箱位于同一台 Exchange 服务器上，Exchange 将把邮件传递给收件人的邮箱。
 - ◇ 如果收件人的邮箱位于另一台 Exchange 服务器上，第一台 Exchange 服务器将把邮件发送给收件人的主邮箱服务器，并由收件人的主邮箱服务器将邮件传递到收件人的邮箱中。



虽然路由组中的所有服务器彼此之间都直接通信，但是当从一个路由组中的服务器必须与另一个路由组中的服务器通信时，则不是直接通信。要允许服务器与其他路由组中的服务器通信，必须创建路由组连接器。虽然可以使用 X.400 连接器或 SMTP 连接器连接路由组，但是路由组连接器是专门为此目的而设计的，并且是连接路由组的首选方法。

在默认情况下，路由组中的所有服务器都可以通过路由组连接器发送邮件。能够通过路由组连接器发送邮件的服务器是“桥头服务器”。每个桥头服务器都是 SMTP 虚拟服务器和 Exchange 服务器的组合，并负责通过连接器传递所有邮件。

如果在如图 6-33 所示的对话框中选择了“显示管理组”复选项，则可以在 Exchange 系统管理器中显示管理组。但如果拥有多个管理组，并且是在纯模式下操作 Exchange Server 2003，则此复选框将不可用，因为管理组会自动显示。如果选择“显示路由组”复选项，则

可以在“管理组”容器中显示路由组（代替“连接器”）。在“路由组”上单击鼠标右键，将显示用于添加或删除路由组的菜单选项。同时选择了以上两个复选项后的系统管理器界面如图 6-34 所示，对比图 6-1 即可见这两个复选项的作用了。

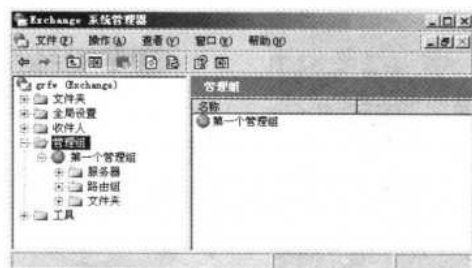


图 6-34 显示了管理组和路由组后的 Exchange Server 2003 系统管理器

(2) 单击【更改模式】按钮，可以改变当前邮件服务器的工作模式。它有两种选择“混合模式”和“纯模式”，混合模式就是包括了以前版本的邮件域，而纯模式就是仅包含 Exchange Server 2003 的邮件域。如果原来为混合模式，更改成纯模式后就无法再撤销，一定要小心操作。确认后系统便自动更改。但不能从纯模式下更改为混合模式。

在 Exchange 组织的默认配置中，只存在一个管理组。可以将所有服务器安装到这一个管理组中（这在集中式管理模型中很有用），也可以创建其他管理组并将服务器安装到相应的管理组中（基于管理模型）。可以重命名“第一个管理组”，并添加新的系统容器，但是不能从该组的“服务器”容器中删除服务器。

只能在安装服务器的过程中将其添加到管理组中。最好是在组织中的第一台 Exchange 服务器上创建必要的管理组，然后将其他服务器安装到相应的管理组中。永远不能在管理组之间移动服务器。但在如图 6-34 所示的对话框中选择了“显示管理组”复选项后还可以新建管理组。方法是在“管理组”子节点上单击鼠标右键，在弹出的快捷菜单中选择【新建】→【管理组】命令。新建管理组后，可以将一个管理组中的一些对象移动到另一个组。如“系统策略”、“公用文件夹”和“路由组成员服务器”（仅限于纯模式）。但是，另外一些对象是不能移动的，如“服务器”和“容器”。只能在相同类型的容器之间移动对象。例如，可以将系统策略从一个系统策略容器移动到另一个管理组中的另一个系统策略容器，但是不能将系统策略移动到公用文件夹容器中。这种类型的操作默认情况下被禁止。具体不作介绍。

6.3.2 “全局设置”节点属性配置

介绍完根节点属性配置外，再来介绍 Exchange Server 2003 邮件服务器的其他主要节点属性的配置。它们关系到整个邮件服务器系统的属性配置。本节首先介绍“全局设置”节点下的“邮件传递”属性设置。

(1) 在如图 6-1 所示主界面的“邮件传递”子节点上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 6-35 所示的对话框。如果该 Exchange Server 2003 邮件服务器中要接收来自其他邮件服务器（包括网络内部和网络外部）发来的邮件，则需要在这里配置这些其他 SMTP 邮件服务器的 IP 地址。方法是在其中单击【添加】按钮，打开如图 6-36

所示的对话框。然后再单击【添加】按钮，打开如图 6-37 所示的对话框。

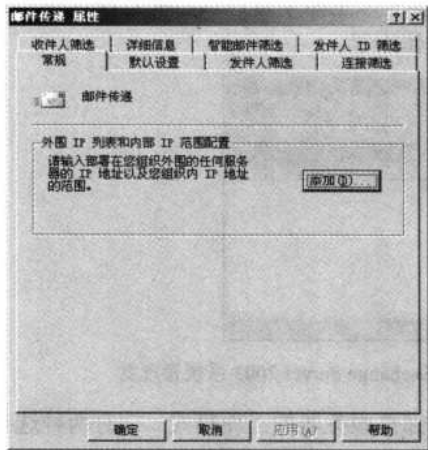


图 6-35 “邮件传递属性”对话框
“常规”选项卡

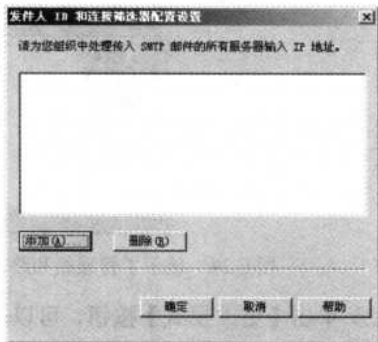


图 6-36 “发件人 ID 和连接筛选器配置设置”对话框

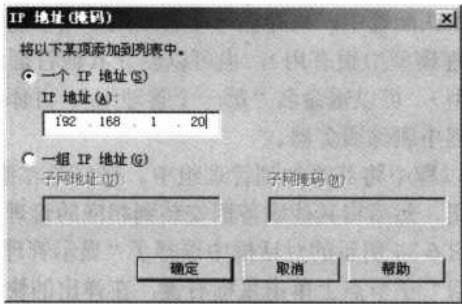


图 6-37 “IP 地址（掩码）”对话框

如果添加的只是一个独立的 SMTP 服务器，则选择“一个 IP 地址”单选项，然后在下面的“IP 地址”栏中输入对应 SMTP 服务器的 IP 地址，可以是网络内部的，也可以是外部网络的。当然如果是外部网络的，则还需要配置路由功能。

如果要添加多个 IP 地址连接的 SMTP 服务器，则可选择“一组 IP 地址”单选项，然后在下面输入这些 SMTP 服务器的网络 IP 地址，然后在“子网掩码”中输入相应的子网掩码。由子网掩码确定他们所在的子网。

完成后再依次单击【确定】按钮完成 SMTP 服务器添加。

(2) 在如图 6-35 所示的对话框中选择“默认设置”选项卡，如图 6-38 所示。在这里可以设置用户可以发送和接收的邮件大小限制（默认为 10MB），以及单一邮件同时发送的接收邮件人数限制。

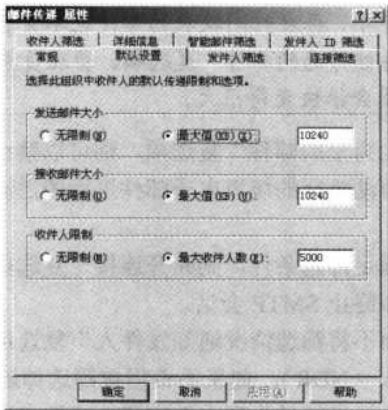


图 6-38 “邮件传递属性”对话框“默认设置”选项卡

如果此服务器上的用户试图发送的某个邮件的收件人数目超过了最大收件人数目，此邮件将作为无法传递的邮件退回给该用户。默认情况下，每个电子邮件的最大收件人数目为 5,000，绝大多数情况下是没有任何问题的，除非是非法的群发，否则基本上不可能一封邮件要发给 5000 人接收。发送、接收邮件大小的限制不宜设置过大，否则服务器可能承受不了。

(3) 单击“发件人筛选”选项卡，如图 6-39 所示。使用此选项卡可以禁止传递特定用户发送的邮件。可以添加或更改要筛选掉的电子邮件地址，或者从列表中删除电子邮件地址；也可以配置特定的筛选选项。使用这些选项可以防止将垃圾邮件或其他不必要的邮件传递给此服务器上的用户。

使用“发件人”列表可以管理要筛选掉的电子邮件地址。如果使用出现在此列表中的电子邮件地址或显示名向该 Exchange 服务器发送电子邮件，电子邮件将不会传递给收件人。发件人地址添加的方法是单击对话框中的【添加】按钮，打开如图 6-40 所示的对话框。在其中要输入相应用户的邮箱地址，实际上就是用户的 SMTP 邮箱地址。还可以使用通配符来阻挡整个用户组。例如，如果要筛选掉来自 contoso.com 域的所有邮件，可键入*@contoso.com。

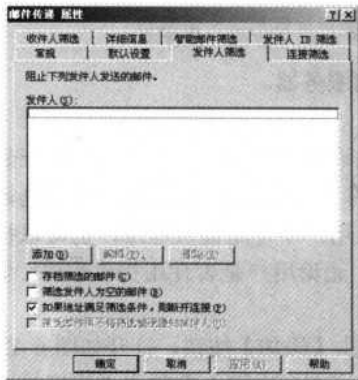


图 6-39 “邮件传递属性”对话框“发件人筛选”选项卡

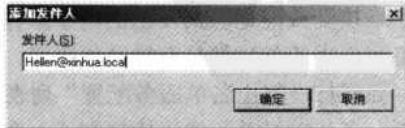


图 6-40 “添加发件人”对话框

如果在如图 6-39 所示的对话框中选择了“存档筛选的邮件”复选项，则可以将“发件人”列表筛选掉的邮件存档。在默认情况下，此选项是不启用的。

注意 在存档邮件中，存在时间较长的邮件也不会自动从存档文件中删除，所以如果选择了“存档筛选的邮件”复选项，管理员要定期清理这些存档邮件，否则存档文件可能会很快变得很大。

如果选择了“筛选发件人为空的邮件”复选项，则可以禁止传递“发件人”这一行为空的邮件，这主要是针对那些自动执行的垃圾电子邮件进行的过滤设置。默认情况下，此选项是不启用的。

如果选择了“如果地址满足筛选条件，则断开连接”复选项，则可以在发件人的地址与筛选器上的地址匹配时，立即终止 SMTP 会话。

如果选择了“接受邮件而不将筛选情况通知发件人”复选项，则可以禁止向被筛选掉的邮件的发件人发送未送达报告（NDR）。如果不希望被筛选掉的电子邮件的发件人得知其邮件未传递，可以使用此选项。如果经常收到大量应筛选掉的邮件，选中此复选项可以改善网络和服务器的性能。

（4）单击如图 6-39 所示的对话框中的“连接筛选”选项卡，如图 6-41 所示。使用该对话框可以创建用于阻塞下列连接 SMTP 服务器的 IP 地址的连接筛选规则。

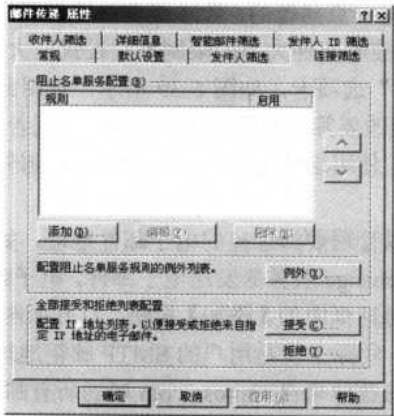


图 6-41 “邮件传递属性”对话框“连接筛选”选项卡

- 在阻止名单提供商所维护的列表中找到服务器。
- 在全局拒绝列表中配置的服务器。

如果你使用阻止名单提供程序，则连接筛选允许用户根据该提供程序的列表来检查传入 IP 地址是否属于要筛选的类别。如果连接服务器的 IP 地址出现在该列表中，则该提供程序将返回一个指示肯定匹配的状态码或位掩码。如果用户不使用提供程序，仍可以指定用户希望始终接受或拒绝从其发出的电子邮件的 IP 地址。无论用户是否使用提供程序，全局接受或拒绝列表中的条目都具有较高优先级。

要添加“阻止名单服务配置”列表，则只需单击【添加】按钮，打开如图 6-42 所示的对话框，在其中可以新建连接规则了。在“显示名”文本框中键入希望在“连接筛选规则”选项卡上的列表中显示的连接筛选规则名称。在“提供程序的 DNS 后缀”文本框中输入提供商附加到 IP 地址的 DNS 后缀。由用户的提供商应提供此信息。单击【来自提供程序服务的返回状态代码】按钮，打开如图 6-43 所示的对话框，在这里可以配置作为筛选依据的返回状

态代码。使用“返回状态代码”对话框可以配置作为规则筛选依据的返回状态代码。

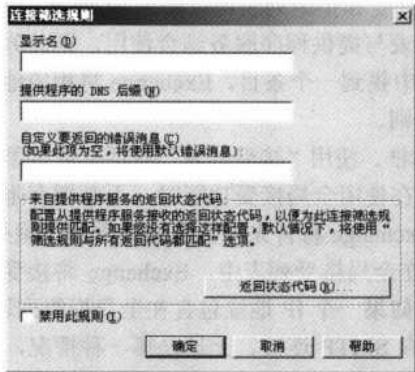


图 6-42 “连接筛选规则”对话框

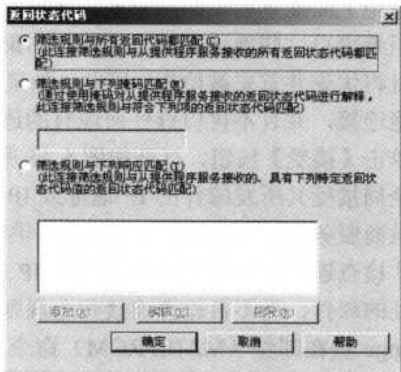


图 6-43 “返回状态代码”对话框

如果选择“筛选规则与所有返回代码都匹配”单选项，则可以将所有返回码与筛选规则进行匹配。如果一个 IP 地址包含在某个列表中，阻止名单提供商服务将发送一个肯定的返回码，然后筛选规则将阻止该 IP 地址。

如果选择“筛选规则与下列掩码匹配”单选项，则可在下面的文本框中输入要使用的掩码，以便解释来自阻止名单提供商服务的返回状态码，以确定提供商的掩码中所使用的约定。

选择“筛选规则与下列响应匹配”单选项，如果要将该筛选规则与多个返回状态码之一进行匹配，则请输入希望该规则与其匹配的返回状态码。例如，如果要检查当 IP 地址包含在“已知的未经请求的商业电子邮件的发件人”列表或“拨号用户”列表中时返回的状态码，则可以使用此选项。

在如图 6-41 所示的对话框的“配置阻止名单服务规则的例外表”栏中单击【例外】按钮，可打开如图 6-44 所示的对话框。在这里可以将 SMTP 地址作为例外添加到连接规则中。无论该地址是否出现在阻止名单提供程序的列表中，只要该地址出现在例外列表中，Exchange 就将接受来自该 SMTP 地址的邮件。可单击对话框中的【添加】按钮，打开类似如图 6-40 所示的对话框（不过此时输入的是收件人地址），请键入单个电子邮件地址，或使用通配符接受特定域中的所有用户。例如，若要筛选掉来自 contoso.com 域的所有邮件，请键入*@contoso.com。

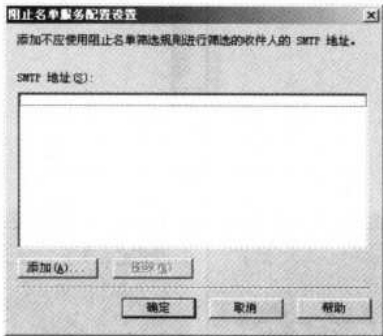


图 6-44 “阻止名单服务配置设置”对话框

344 网管员必读——网络应用（第2版）

如果在如图 6-41 所示的对话框的“全部接受和拒绝列表配置”栏中可以配置全部接受，或者拒绝上面配置列表的邮箱账户名单。使用全局接受和拒绝列表可以添加 IP 地址，以便接受或拒绝来自这些地址的所有邮件。如果将这些列表与提供程序服务结合使用，则此列表中的条目将优先并首先被检查。因此，如果在此列表中找到一个条目，Exchange 将相应地接受或拒绝连接，并且不再检查任何现有的连接筛选规则。

单击【接受】按钮，打开如图 6-45 所示的对话框。使用“接受列表”对话框可以添加你希望全局接受其所发邮件的 IP 地址或 IP 地址组。在使用全局接受功能时，不必拥有阻止名单提供商服务。如果使用了阻止名单提供商服务，Exchange 将首先检查全局接受和拒绝列表，然后才检查连接筛选规则。如果一个 IP 地址包含在全局接受列表中，Exchange 将接受来自该地址的邮件，而不再检查连接筛选规则。同样，如果一个 IP 地址包含在全局拒绝列表中，Exchange 将在邮件（MAILFROM）命令发出后丢弃 SMTP 连接。无论是哪一种情况，只要 Exchange 发现一个 IP 地址包含在这两个全局列表的一个列表中，它就不再检查连接筛选规则。在“IP 地址（掩码）”列表中可以添加或删除用户希望全局接受的 IP 地址或 IP 地址组。Exchange 将首先检查全局接受列表，并且在发现一个 IP 地址包含在该列表中时，自动接受传入的连接。

如果单击如图 6-41 所示的对话框中的【拒绝】按钮，打开如图 6-46 所示的对话框。使用“拒绝列表”对话框可以添加用户希望全局拒绝其所发邮件的 IP 地址或 IP 地址组。在使用全局接受或拒绝列表时，不必拥有阻止名单提供商服务。如果确实使用阻止名单提供商服务，Exchange 将首先检查全局拒绝和接受列表，然后才检查连接筛选规则。如果一个 IP 地址包含在全局拒绝列表中，Exchange 将在邮件（MAILFROM）命令发出后丢弃 SMTP 连接。同样，如果一个 IP 地址包含在全局接受列表中，Exchange 将接受通信，而不再检查连接筛选规则。无论是哪一种情况，只要 Exchange 发现一个 IP 地址包含在这两个全局列表的一个列表中，它就不再检查连接筛选规则。在“IP 地址（掩码）”列表中可以添加或删除用户希望全局拒绝的 IP 地址或 IP 地址组。Exchange 将首先检查全局拒绝列表，并且在发现一个 IP 地址包含在该列表中时，自动拒绝传入的连接。

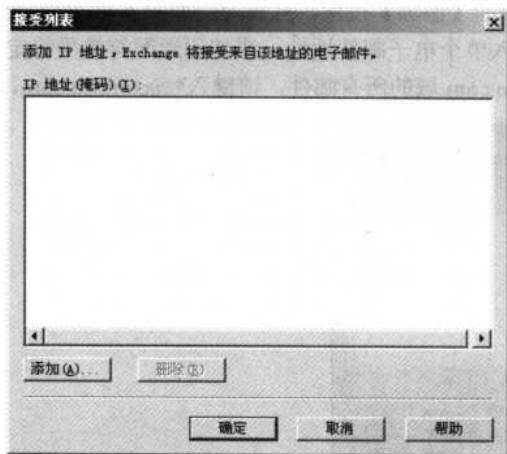


图 6-45 “接受列表”对话框

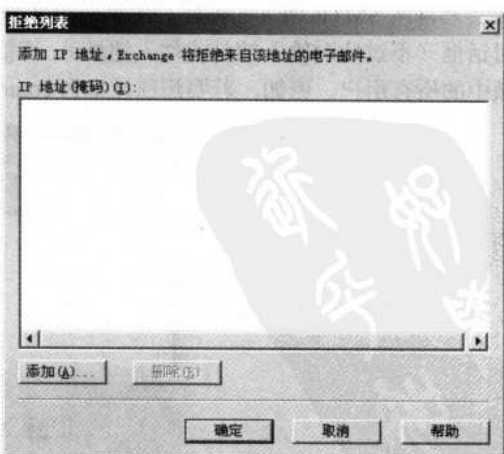


图 6-46 “拒绝列表”对话框

注意 连接筛选规则只应用于匿名连接。已通过身份验证的用户和 Exchange 服务器将绕过这些验证。同时，全局接受列表优先于全局拒绝列表。例如，若希望阻塞来自一组 IP 地址的邮件，但同时又希望接受来自该组中某个特定 IP 地址的邮件。要做到这一点，请在全局拒绝列表中输入子网和掩码以阻塞该组 IP 地址，然后在全局接受列表中添加希望从其接受邮件的单个 IP 地址。因为全局接受列表优先于全局拒绝列表，所以 Exchange 将接受来自该 IP 地址的邮件。

另外，创建连接筛选规则以后，必须将该规则应用于希望使用该规则的 SMTP 虚拟服务器。请对 SMTP 虚拟服务器属性应用该连接筛选器。具体设置方法参见下面的图 6-51 所对应的介绍。

(5) 在如图 6-41 所示的对话框中选择“发件人筛选”选项卡，如图 6-47 所示。使用“收件人筛选”选项卡可以禁止传递被发送到特定收件人地址的邮件。具体来说，使用此选项卡完成以下任务。

- 将发送到你的 Active Directory 中不包含的用户的电子邮件筛选掉。
- 将发送到任何收件人（无论地址是否有效）的电子邮件筛选掉。例如，如果一个电子邮件被发送到恰当定义的收件人，并且该邮件是未经请求的商业电子邮件，则可以阻塞该电子邮件。

注意 收件人筛选规则只应用于匿名连接。已通过身份验证的用户和 Exchange 服务器将绕过这些验证。

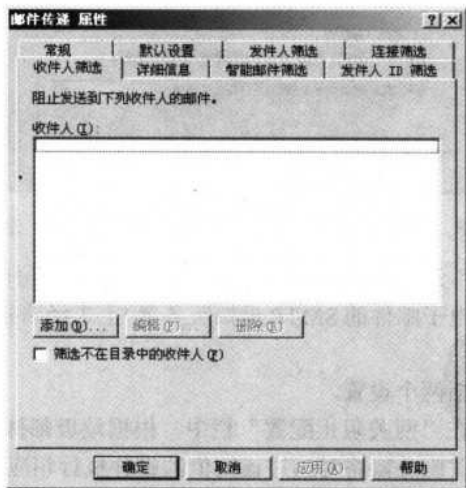


图 6-47 “邮件传递属性”对话框“收件人筛选”选项卡

使用“收件人”列表可以管理要筛选掉的电子邮件地址。如果邮件被发送到出现在此列表中的电子邮件地址或显示名，则该电子邮件将不会传递给收件人。单击【添加】按钮，打开类似如图 6-38 所示的对话框，可以向列表中添加电子邮件地址。可以键入单个电子邮件地址，或者使用通配符来阻塞整组收件人。例如，若要筛选掉发往 contoso.com 域的所有邮件，

可键入*@contoso.com。

选中“筛选不在目录中的收件人”复选框，则可以将发往 Active Directory 中不包含的用户电子邮件筛选掉。在默认情况下，此选项是不启用的。Exchange 仅执行 Active Directory 查找，并且阻塞发往特定域（传入邮件在该域上经过授权）的传入邮件的无效收件人。此设置在收件人策略中进行配置，具体参见本章后面的相关内容。



警告

启用此复选项时，有可能使未经请求的商业电子邮件的发件人在 Exchange 组织中发现有效的电子邮件地址。这是因为在 SMTP 会话期间，SMTP 虚拟服务器为有效和无效的收件人发送不同的响应。有关收件人筛选在 SMTP 虚拟服务器上的启用也请参见下面将要介绍的图 6-51 所对应的设置。

(6) 在如图 6-41 所示的对话框中选择“智能邮件筛选”选项卡，如图 6-48 所示。这是 SP2 补丁新增的功能。

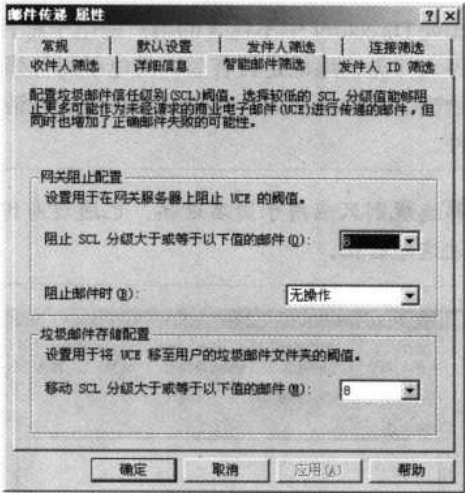


图 6-48 “邮件传递属性”对话框“智能邮件筛选”选项卡

使用“智能邮件筛选”选项卡配置 Exchange 使用的设置，可以阻止网关 SMTP 虚拟服务器(接受传入的 Internet 电子邮件的 SMTP 虚拟服务器)上未经请求的商业电子邮件(UCE)，也称为垃圾邮件。

配置智能邮件筛选包括两个设置。

- 网关阻止配置：在“网关阻止配置”栏中，根据垃圾邮件信任级别（SCL）分级确定一个阈值。网关服务器将对超过该阈值的邮件执行相应的操作。还可以定义用户希望网关执行的操作类型。
- 垃圾邮件存储配置：在“垃圾邮件存储配置”栏中，根据 SCL 分级定义一个阈值。Microsoft Exchange 2003 邮箱存储将使用该阈值确定应将邮件传递到用户的收件箱中还是用户的垃圾邮件文件夹中。

若要筛选未经请求的商业电子邮件（UCE），必须在接收传入 Internet 电子邮件的所有 SMTP 虚拟服务器上启用智能邮件筛选，而不需要启用 Exchange 邮箱服务器中 SMTP 虚拟服

务器上的智能邮件筛选。如果启用了网关 SMTP 虚拟服务器上的智能邮件筛选，则 Exchange 邮箱服务器将 SCL 分级随每个传入的 Internet 电子邮件一起接收，并执行相应的操作。

在 SMTP 虚拟服务器上的智能邮件筛选的方法是在相应 SMTP 邮件服务器中（Exchange Server 2003 系统管理器中）单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择【常规】命令，如图 6-49 所示。

单击【高级】按钮，打开如图 6-50 所示的对话框。然后选择一个标识项，单击【编辑】按钮，打开如图 6-51 所示的对话框。选中“应用智能邮件筛选器”复选项，再单击【确定】按钮。在“高级”对话框中的“已启用筛选器”列下会显示出“是”状态。若要禁用筛选功能，请清除“应用智能邮件筛选器”复选项。

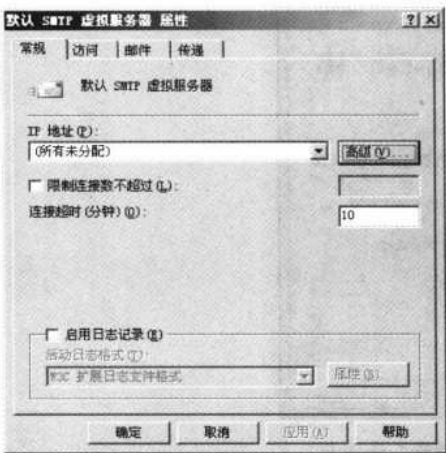


图 6-49 “默认 SMTP 虚拟服务器属性”对话框“常规”选项卡

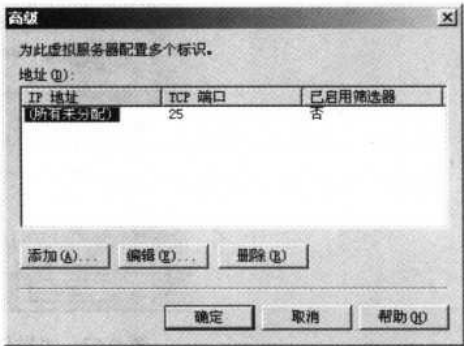


图 6-50 “高级”选项卡

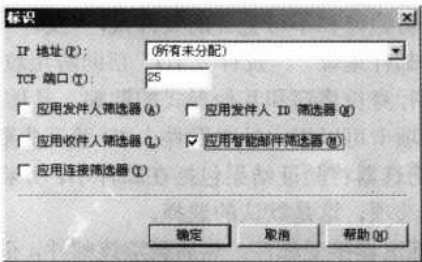


图 6-51 “标识”对话框



从如图 6-51 所示的对话框中可以看出，在这里还可以在 SMTP 服务器配置是否启用前面介绍的“发件人筛选”、“收件人筛选”、“连接器筛选”和下面将要介绍的“发件人 ID 筛选”过滤设置。

在 SMTP 虚拟服务器上启用智能邮件筛选后，智能邮件筛选将基于该邮件是垃圾邮件的可能性对每个传入的 Internet 邮件进行评估并分配邮件分级。不管设置的分级阈值如何，所有传入的邮件都以 SCL 分级标记。此分级将与其他邮件属性一起保存，并且这些属性将随邮

件一起发送到其他 Exchange 服务器。在“网关阻止配置”下的“阻止 SCL 分级大于或等于以下值的邮件”中选择分级。智能邮件筛选将对超过该分级的邮件执行相应操作。邮件标记的分级超出指定阈值时，智能邮件筛选将基于“阻止邮件时”中指定的选择对邮件执行相应操作。

Exchange 邮箱服务器使用阈值及“垃圾邮件存储配置”中指定的设置来确定将邮件传递到用户的收件箱还是垃圾邮件文件夹。

(7) 在如图 6-41 所示的对话框中选择“发件人 ID 筛选”选项卡，如图 6-52 所示。这也是 SP2 补丁新增的功能。

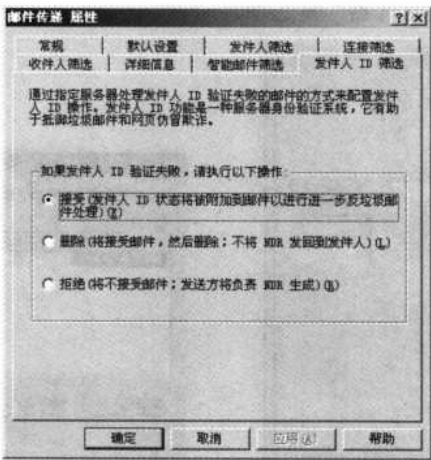


图 6-52 “发件人 ID 筛选”选项卡

“发件人 ID”功能是一种业界标准的服务器身份验证系统，可用来对未经请求的商业电子邮件（UCE）和网页仿冒欺诈提供更大的保护。发件人 ID 功能有助于抵制垃圾邮件和网页仿冒欺骗。为了帮助区分可验证和不可验证的发件人，“发件人 ID”将根据实际的发送地址检查和验证发件人的电子邮件地址。“发件人 ID”帮助防止垃圾邮件发送者“哄骗”或伪造合法的电子邮件地址以进行身份盗窃和其他形式的欺骗。具体的发件人 ID 筛选在 SMTP 虚拟服务器中配置。在本选项卡可以指定针对发件人 ID 验证失败时可进行以下具体操作。

- 如果要发件人 ID 筛选器将验证结果包括在邮件中，并将该邮件传递到用户的邮箱，则选择“接受”单选项，这是默认的选择。
- 如果要发件人 ID 筛选器接受邮件，然后删除该邮件，而不向用户发送未送达报告，则选择“删除”单选项。
- 如果要发件人 ID 筛选器在 SMTP 协议级拒绝邮件，并向用户发送 NDR 邮件，则选择“拒绝”单选项。



注意

若要使用“发件人 ID”筛选，必须在接收传入 Internet 电子邮件的所有 SMTP 虚拟服务器上启用“发件人 ID”筛选，但不需要启用 Exchange 邮箱服务器中 SMTP 虚拟服务器上的“发件人 ID”，如图 6-51 所示。

6.4 邮件服务器属性设置

在邮件服务器属性设置中可以设置的设置包括启用邮件跟踪、为客户端配置语言支持、安排邮箱管理进程、使用诊断日志记录解决特定的问题、使用公用文件夹引用和目录访问选项，以及对于管理 Exchange 服务器而言很重要的其他设置。还可以在单个服务器的基础上管理协议设置、服务以及备份和还原过程等。

1. 常规属性设置

在如图 6-1 所示系统管理器控制台“管理组”（启用了“管理组”功能时）节中“服务器”节点下选择相应的邮件服务器，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 6-53 所示的对话框。在这里有 12 个选项卡，本节所要介绍的配置都在“常规”选项卡中。



图 6-53 “常规”选项卡

在“常规”选项卡中可以启用主题日志记录、邮件跟踪、日志文件目录和前端服务器等属性。通过启用主题日志记录和显示，可以在邮件跟踪中心存储电子邮件主题，以便可以通过该中心查看邮件。通过启用邮件跟踪，可以将邮件存储在邮件跟踪日志文件中。在默认情况下，日志文件每七天删除一次。

邮件跟踪中心在混合模式和纯模式 Exchange 组织中的服务器之间跟踪邮件。邮件跟踪中心也可以跟踪与另一个邮件系统（如 Lotus Notes）之间来往的邮件。通过邮件跟踪中心，可以搜索所有种类的邮件，包括系统邮件（发生问题时显示的警报）、公用文件夹邮件及电子邮件。要使服务器的邮件出现在邮件跟踪中心，必须先在 Exchange 服务器上启用主题日志记录。但是，启用这种类型的日志记录会导致如下结果：简单邮件传输协议（SMTP）和 MAPI 队列中邮件的主题行将显示在队列查看器的“主题”列中。在默认情况下，出于保密目的，“主题”列保留为空（例如，一些 Exchange 组织希望防止较低级别的管理员查看邮件主题。）因此，在启用主题日志记录之前，应验证所在组织是否有关于显示主题行信息的策略。使服务器的邮件出现在邮件跟踪中心的方法是在如图 6-53 所示的对话框中选择“启用主

350 网管员必读——网络应用（第2版）

题日志记录和显示”复选项，可以将邮件主题存储在邮件跟踪日志文件中。



如果“启用主题日志记录和显示”复选项不可用（或显示为灰色），则说明存在应用于该服务器的服务器策略对象。必须在该策略上启用主题日志记录和显示，或者将服务器从该策略中删除。要查看应用于该服务器的策略，请查看“策略”选项卡，具体将在本节后面介绍。

如果选择“启用邮件跟踪”复选项，则可跟踪此服务器上所有邮件组件的邮件。可以创建服务器策略，以便控制管理组中一组服务器的邮件跟踪选项。不过，也可以单个服务器为基础，启用邮件跟踪。例如，你不想跟踪所有服务器上的邮件，但是特定 Exchange 服务器上的用户遇到了邮件流问题，那么可以在出现邮件流问题的服务器上启用邮件跟踪。或者，可以只跟踪 Internet 网关服务器上的邮件。

在单个服务器上启用邮件跟踪时，通过该服务器路由的邮件将添加到邮件跟踪日志中。这些日志是文本文件，可以通过检查日志来监视并排除邮件流故障。这些日志文件由每台服务器上的 Exchange 系统助理服务维护。



如果“启用邮件跟踪”复选项不可用（或显示为灰色），则说明存在应用于该服务器的服务器策略对象。必须在该策略上启用邮件跟踪，或者将服务器从该策略中删除。要查看应用于该服务器的策略，请查看“策略”选项卡，具体将在本节后面介绍。

如果启用邮件跟踪，可能需要自定义 Exchange 管理所生成日志文件的方式。在默认情况下，Exchange 将邮件跟踪日志文件存储在系统盘的 Program Files\Exchsrvr 文件夹中，并且每七天删除这些日志文件一次。这些默认设置也许能也许不能满足用户 Exchange 环境的要求。要指定邮件跟踪日志文件的路径和文件夹，可以在“常规”选项卡上的“日志文件目录”文本框中配置。更改日志文件目录的路径后，Exchange 将以后的日志文件保存到新的路径下。但是，Exchange 不会将现有的日志文件移动到新的位置。此项操作必须由用户手动完成。

如果允许日志文件在服务器上累积，它们将消耗大量的磁盘空间，并且可能会影响性能。所以应定期审查和删除日志文件。但是，要确保使日志文件在服务器上保留足够长的时间，以便出现邮件流问题时，可以检查这些文件。也可以将日志文件移动到具有容纳更多日志文件的带宽的另一个磁盘上，这是一项额外的工作，方法是先选择“删除日志文件”复选项，然后在“删除超过以下时间的文件（天）”文本框中，键入文件在被删除前要在服务器上保留的天数。

如果选择“这是前端服务器”复选项，可以将当前服务器配置为前端服务器。将某台服务器配置为前端服务器时，通常指定该服务器专门接收来自邮件客户端（如 HTTP、Internet 邮件访问协议版本 4（IMAP4），以及邮局协议版本 3（POP3））的请求，并将客户端请求中继到相应的后端服务器。Exchange 前端服务器需要的服务取决于用户在该服务器上使用的协议，以及是否要在初始安装后进行配置更改。

将某台服务器指定为前端服务器后，应在该服务器上删除任何不重要的组件，或禁用任何不必要的服务。删除这些组件或禁用这些服务使得前端服务器可以更高效地中继客户端请求，并由于减少了易于受到攻击的服务或组件数而提高了安全性。尤其是可以从 Exchange 前端服务器上删除公用文件夹存储和存储组。此外，如果前端用户不使用 SMTP 发送邮件，

还可以从前端服务器上删除邮箱存储。要停止或禁用服务，可在“服务”管理单元进行。

如果选择“自动将致命的服务错误信息发送到 Microsoft”复选项，可以在发生致命错误时，通过安全连接向 Microsoft 发送错误报告。发送到 Microsoft 的错误报告是通过 Secure HTTP (HTTPS) 发送的，这是比 HTTP 更安全的通道。要发送报告，服务器必须能够通过 HTTP 访问 Internet。

2. 区域属性设置

区域设置其实就是语言设置，让 Exchange 支持所需的各种语言。

单击如图 6-53 所示的对话框中的“区域设置”选项卡，如图 6-54 所示。之所以要设置“区域设置”，是因为不同国家和地区在日期、时间和货币等信息的格式和表示方面有不同的习惯。为了适应这些区别，应使用“区域设置”选项卡来定义如何显示日期、货币和时间值，并定义如何控制诸如排序顺序等其他国际设置。

对于“区域设置”选项卡中列出的每个区域设置，服务器都能够为客户端提供按照该区域设置中使用的约定排序和设置格式的数据。例如，如果该列表中出现“印地语”，连接到该服务器的印地语客户端将看到按照印地语的习惯排序和设置格式的信息。

国内用户安装的是简体中文语言版本，所以默认显示的是“中文（中国）”，要添加其他语言设置（在外资企业中是经常需要的），单击【添加】按钮，打开如图 6-55 所示的对话框。

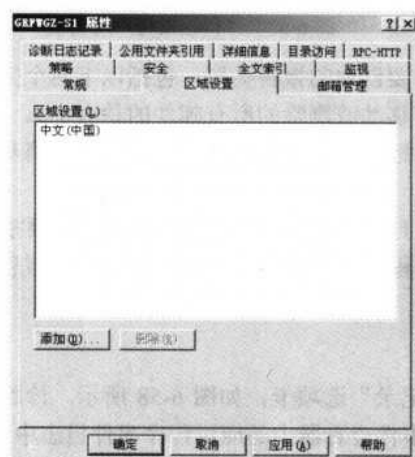


图 6-54 “区域设置”选项卡

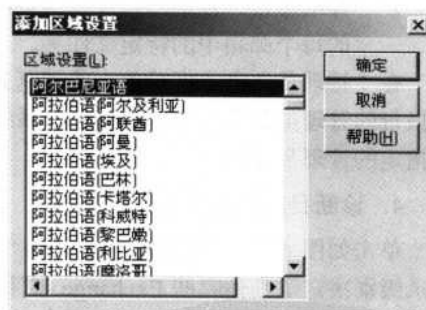


图 6-55 “添加区域设置”对话框

3. 邮箱管理属性设置

单击如图 6-54 所示的对话框中的“邮箱管理”选项卡，如图 6-56 所示。在这里可以设置是否运行邮箱管理进程、是否发送邮箱管理报告和接受管理报告的邮箱管理员。

在“启动邮箱管理进程”下拉列表框中，根据关联的收件人策略指定的规则，选择邮箱管理进程何时启动（在该特定服务器上），也就是选择一个日程安排。与该服务器关联的收件人策略确定了邮箱管理器将清理哪些邮箱。还可以根据组织的要求来自定义邮箱管理日程安排。例如，可以创建一个自定义日程安排，使邮箱管理器在星期六午夜运行。方法是单击其中的【自定义】按钮，在打开的如图 6-57 所示的对话框中定义邮箱管理进程运行的日程安排。安排邮箱管理器的日程时，可以指定接收邮箱管理器报告的邮箱。还可以选择要生成的

352 网管员必读——网络应用（第2版）

报告的类型。报告可以包括不同类型的信息，例如邮箱管理器何时运行、应用了哪些邮箱收件人策略、处理了哪些邮箱、处理了哪些文件夹、移动或删除的邮箱数，以及移动或删除的邮件大小。

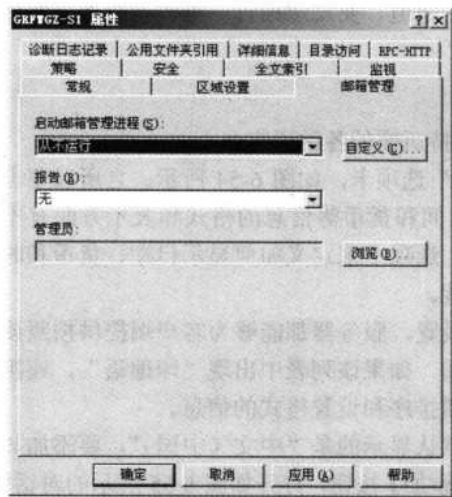


图 6-56 “邮箱管理”选项卡

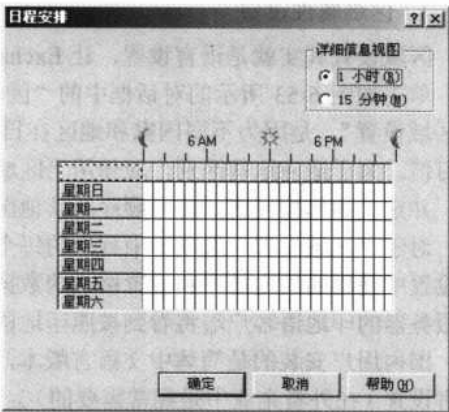


图 6-57 “日程安排”对话框

在“报告”下拉列表框中无论何时处理邮箱都要创建的报告类型，包括以下两个方面。

- 摘要报告：包含基本信息（如邮箱管理器移动或删除的所有邮件的总大小）。
- 详细报告：包括邮箱管理器每次运行时所运行的特定策略、处理的特定邮箱及处理的每个邮箱中的特定文件夹。

在“管理员”文本框后单击【浏览】按钮，在打开的对话框中可以选择组织中要接收这些报告的管理员邮箱。这样设置后，系统会根据日程安排自动把所设置的报告项目信息发送到指定的管理员邮箱中。

4. 诊断日志记录属性设置

单击如图 6-56 所示的对话框中的“诊断日志记录”选项卡，如图 6-58 所示。诊断日志记录级别决定了其他哪些 Exchange 事件会写入到事件查看器中的应用程序事件日志中。事件查看器是 Windows Server 2003 中的一个组件，可以用来监视硬件和软件活动。可以使用诊断日志记录来记录与身份验证、连接，以及用户操作有关的重大事件。

配置诊断日志记录的第一步是确定必须对 Exchange 服务器上的哪些服务启用诊断日志记录。应分别对每台服务器上的每个服务配置诊断日志记录。例如，如果在单个虚拟服务器上启用了协议日志记录，那么该设置只是确定了运行该虚拟服务器的 Exchange 服务器对该协议的日志记录功能。

在对话框左边的“服务”窗口中选择要配置的相应服务后，下一步应为这些服务设置日志记录级别。根据详细程度，划分为 4 个日志记录级别：“最高”为记录日志记录级别小于或等于 5 的事件；“中等”为记录日志记录级别小于或等于 3 的事件；“最低”为记录日志记录级别小于或等于 1 的事件；“无”只记录关键事件、错误事件和日志记录级别等于 0 的事件。当 Exchange 生成的事件低于或等于该日志记录级别时，该事件即被记录下来。事件范围

比较广，从重大事件（如应用程序失败），到较重大的事件（如收到通过网关传送的邮件），再到仅仅与调试有关的事件都包括在内，通常只记录关键事件。但是，当发生问题时，可以更改诊断日志记录的日志记录级别，以捕获更多更详细的事件。



图 6-58 “诊断日志记录”选项卡



注意

应分别对每台服务器上的每个服务配置诊断日志记录。例如，如果在单个虚拟服务器上启用了协议日志记录，那么该设置只是确定了运行该虚拟服务器的 Exchange 服务器对该协议的日志记录功能。

5. 公用文件夹引用属性设置

单击如图 6-58 所示的对话框中的“公用文件夹引用”选项卡，如图 6-59 所示。



图 6-59 “公用文件夹引用”选项卡

当用户连接到不包含其他人正在查找的公用文件夹内容副本的公用文件夹存储时，Exchange 会将该用户重定向到包含该内容副本的另一个公用文件夹存储。在默认情况下，Exchange 试图将用户重定向到本地路由组中的服务器。如果这些服务器中没有需要的内容，

Exchange 将按照组织的路由组拓扑来找到相应的服务器。Exchange 使用路由组之间的连接器的开销，基于最有效的路由路径找到相应的服务器。

由于 Exchange 保持路由组之间的可用连接的记录，并尽可能使用最有效的路由，因此建议在“公用文件夹引用选项”下拉列表框中选择“使用路由组”选项来确定 Exchange 如何将用户重定向到另一个公用文件夹。但是，如果必须排除特定服务器的故障，或者正在对网络的某一部分进行维护并希望指定在此维护期间可用的特定服务器，则可以创建一个自定义的公用文件夹引用服务器列表。

自定义的公用文件夹引用列表是 Exchange Server 2003 中的新增功能。在 Exchange 2000 中，只能指定是否允许在路由组之间实现公用文件夹引用。要创建自定义的公用文件夹引用服务器列表，应在“公用文件夹引用选项”下拉列表框中选择“使用自定义列表”选项，激活对话框中的其他按钮，单击【添加】按钮可在打开的对话框中选择其他服务器。当创建自定义服务器列表时，还可以分配开销以便设置引用列表中服务器的优先级。

开销是一种设置公用文件夹引用列表中服务器的优先级的方法。以网络连接和可用带宽作为标准，为组织中的每个连接器定义开销。这样，具有最佳网络连接和最多可用带宽的连接器被分配的开销最低。Exchange 只有在低开销服务器不可用时才使用高开销服务器。

当选择“使用自定义列表”选项并创建可用于引用的服务器列表时，“公用文件夹引用”选项卡将在列表中显示每个服务器的名称，以及与这些服务器关联的所有开销。如果要设置 Exchange 使用所列出的服务器的优先顺序，必须更改与每个服务器关联的开销，并为用户希望 Exchange 先使用的那些服务器分配较低的开销。

6. 目录访问属性设置

单击如图 6-59 所示的对话框中的“目录访问”选项卡，如图 6-60 所示。Exchange 是与 Active Directory 紧密集成在一起的。这种集成要求 Exchange Server 2003 的核心组件访问 Active Directory 中的目录信息。这个“目录访问”（DSAccess）选项卡中的共享组件控制着 Exchange 中的大多数组件如何与 Active Directory 交互。



图 6-60 “目录访问”选项卡

在 Exchange Server 2003 中，DSAccess 是中心机制，它确定 Active Directory 拓扑，打开适当的轻型目录访问协议（LDAP）连接，并排除服务器故障。DSAccess 负责下列功能。

- 从 Active Directory 中检索信息，或向 Active Directory 写入信息，例如配置数据和收件人。
- 缓存 Active Directory 中的信息，以便改善查询 Active Directory 时的性能。DSAccess 在本地缓存配置和收件人数据，以便此信息用于其他 Exchange 服务器的后续查询。在本地缓存信息还具有其他好处，例如防止由于对 Active Directory 的额外查询而导致的网络流量。
- 构建其他 Exchange 组件可以查询的可用域控制器和全局编录服务器列表。例如，MTA 将 LDAP 查询通过 DSAccess 层路由到 Active Directory。
- 为连接到数据库，存储进程使用 DSAccess 从 Active Directory 中获取配置信息。为路由邮件，传输进程使用 DSAccess 获取有关连接器布置的信息。

在上面列出的功能中，用户在服务器上可以控制的唯一功能只涉及可用域控制器和全局编录服务器列表的构建。可以让 DSAccess 自动创建该列表，也可以手动创建此列表以供 DSAccess 使用。

在默认情况下，在每台 Exchange 服务器上，DSAccess 自动在 Active Directory 中检测可用于 Exchange 服务器查询的适当域控制器和全局编录服务器。控制此默认行为的设置该选项卡底部的“自动探查服务器”复选项，选中这个复选项，DSAccess 组件将可以自动探查 Exchange 组织中的下列服务器。

- 配置域控制器：在 Active Directory 配置命名上下文中读取和写入信息的单个域控制器。DSAccess 选择某个域控制器或全局编录服务器来充当配置域控制器。所有配置数据均由此配置域控制器写入和读取。
- 工作域控制器：在本地域中执行 Active Directory 对象查找的域控制器（多达 10 个）。这些域控制器主要用来更新本地域中的对象，或读取未复制到全局编录服务器的非配置数据。
- 工作全局编录服务器：执行目录林范围内查询的全局编录服务器（多达 10 个）。所有用户数据都是在全局编录服务器上查找得到的。

为探查这些服务器，目录访问查找运行 Windows Server 2003 或 Windows 2000 Server Service Pack3（SP3）（或更高版本）的域控制器和全局编录服务器。然后，目录访问测试这些服务器，并选择供 Exchange 服务用来执行 Active Directory 查询的适当服务器。



由于手动构建的拓扑不会自动更新，因此强烈建议用户使用“自动探查服务器”设置。如果在“显示”下拉列表框中选择了“所有域控制器”选项，将无法重新配置“自动探查服务器”复选项。

为解决特定全局编录服务器或域控制器遇到的问题，可能需要通过清除“自动探查服务器”复选项的选择来覆盖服务器的自动探查。例如，要确定对某个全局编录服务器的查询是否工作正常，可以手动将该服务器设置为唯一可用的全局编录服务器。

356 网管员必读——网络应用（第2版）

手动为 DSAccess 创建拓扑时，将不再拥有 DSAccess 自动探查拓扑时所拥有的自动故障转移和负载平衡等优点。如果手动设置的服务器变得不可用，该列表将不会更新，并且 Exchange 仍然尝试使用这个不可用的服务器，从而导致 Exchange 失败。

如果在该选项卡上手动设置的域控制器或全局编录服务器运行的不是 Windows 2000 Server SP3 或更高版本，Exchange 将不会使用该域控制器和全局编录服务器，并且 Exchange 将记录事件。

要手动为目录访问创建拓扑，首先要在“显示”下拉列表框中选择要创建的拓扑结构类型，然后在该选项卡中清除“自动探查服务器”复选项的选择，这将清除当前的服务器列表。单击【添加】按钮，打开如图 6-61 所示的对话框添加服务器，在其中要选择新的服务器类型，单击【确定】按钮即可添加新的目录访问拓扑结构（实际上就是网络中的各类服务器结构）。单击【删除】按钮将已添加的服务器从拓扑中删除。

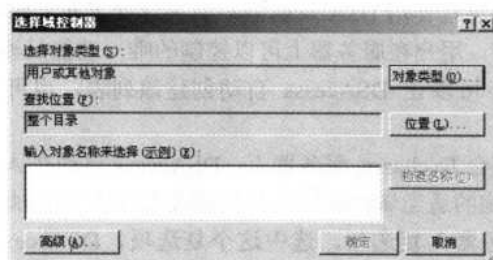


图 6-61 “选择域控制器”对话框

7. RPC-HTTP 属性设置

单击如图 6-60 所示的对话框中的“RPC-HTTP”选项卡，如图 6-62 所示，这是 SP2 新增的功能。使用此选项卡将该服务器配置为 RPC 代理服务器。此功能使该服务器可与运行 Outlook 2003 的客户端计算机进行 RPC over HTTP 通信。

如果选择了“不是 Exchange 管理的 RPC-HTTP 拓扑的一部分”单选项，则从 RPC over HTTP 拓扑删除 Exchange 前端或后端服务器，这是系统默认选择；如果选择了“RPC-HTTP 前端服务器”单选项，则将前端服务器指定为 RPC 代理服务器；如果选择“RPC-HTTP 后端服务器”单选项，则将 Exchange 后端服务器指定为可由 RPC over HTTP 客户端访问。

8. 策略属性设置

单击如图 6-62 所示的对话框中的“策略”选项卡，如图 6-63 所示。系统策略可以灵活地管理大量的 Exchange 服务。系统策略定义应用于一个或多个 Exchange 服务器的设置。例如，可以使用系统策略创建一个统一的方法对一组服务器中的邮件进行跟踪。

由于策略影响一组服务器，因此，在这个选项卡只能查看已应用于该服务器的策略。不能使用该选项卡修改或删除这些策略。要修改或删除已应用于某个特定服务器的系统策略，必须更改该策略本身。具体将在本章后面专门介绍。

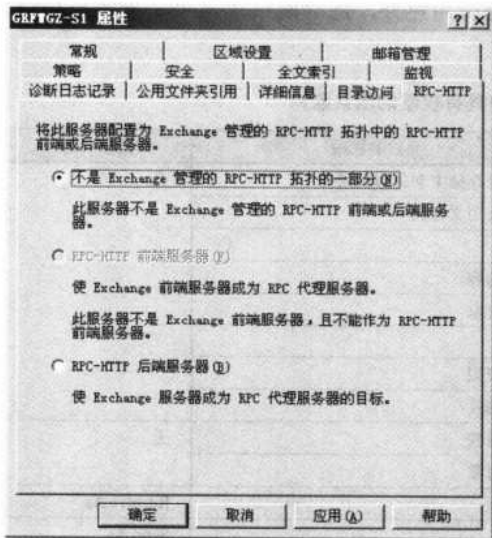


图 6-62 “RPC-HTTP”选项卡

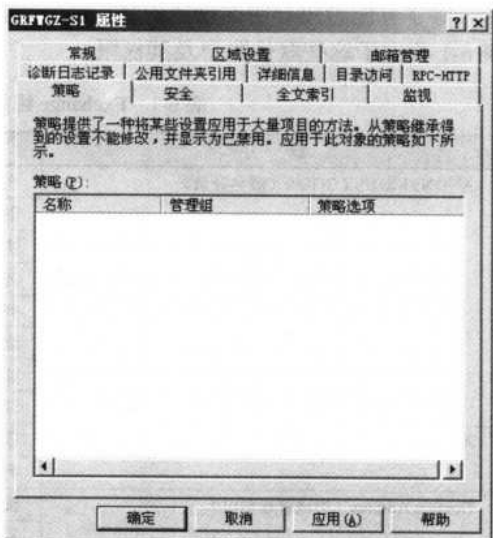


图 6-63 “策略”选项卡

9. 安全属性设置

单击如图 6-63 所示的对话框中的“安全”选项卡，如图 6-64 所示。在这里可以设置各用户，或组对象访问邮件服务器的权限。也可以单独对某些 Exchange 对象设置权限，这些对象包括公用文件夹树、地址列表、邮箱存储、协议，以及服务器。对于这些对象，Exchange 使用并扩展了 Active Directory 权限。像读取、写入和列出内容都是 Active Directory 权限示例。扩展的 Exchange 权限示例有创建公用文件夹和查看信息存储状态。查看对象的权限时，Active Directory 权限出现在列表的上面，其下面是 Exchange 扩展权限。

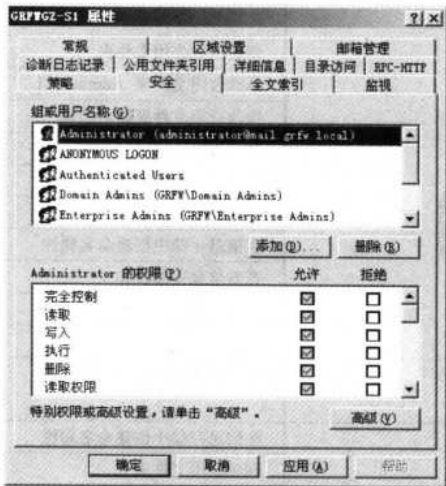


图 6-64 “安全”选项卡

358 网管员必读——网络应用（第2版）

除了分配给用户明确指定的 Exchange 管理员角色外，还分配给了几个系统账户和组，表 6-1 列出了这些默认账户及其权限。

表 6-1 Exchange 组织中具有权限的默认账户

账 户	允许的权限	拒 绝
ANONYMOUS LOGON (匿名登录)	在信息存储中创建命名属性	无
	创建公用文件夹	
	执行	
	列出内容	
	列出对象	
	读取	
	读取权限	
	读取属性	
Authenticated users (经过身份验证的普通用户)	读取属性	无
	列出对象	
Domain Admins (根域管理员组)	读取	Receive As
	写入	Send As
	执行	
	删除	
	读取权限	
	更改权限	
	取得所有权	
	创建子项	
	列出内容	
	自行添加/删除	
	读取属性	
	写入属性	
	列出对象	
	创建公用文件夹	
	创建顶级公用文件夹	
	修改公用文件夹 Admin ACL	
	修改公用文件夹副本列表	
	打开邮件发送队列	
	读取元数据库属性	
	管理信息存储	
	在信息存储中创建命名属性	
	查看信息存储状态	
	Receive As	
	Send As	
Enterprise Admins (企业管理员组)	完全控制	Receive As
		Send As
Everyone (每个人组)	在信息存储中创建命名属性	无
	创建公用文件夹	
	执行	
	列出内容	

(续表)

账 户	允许的权限	拒 绝
	列出对象	
	读取	
	读取权限	
	读取属性	
Exchange Domain Servers (Exchange 邮件域服务器组)	完全控制	无

大多数权限设置都是 Exchange 组织对象从配置目录分区层次结构中的父容器那里继承的。例如，Enterprise Administrators 在配置目录分区的根容器被授予了完全控制权限。由于权限在默认情况下由配置目录分区中的所有子对象（包括 Exchange 组织容器）继承，因此 Enterprise Administrators 也是 Exchange 管理员（完全控制）。

在默认情况下，Exchange 中的权限是继承的。例如，特定服务器包含的对象（如该服务器上的公用文件夹和邮箱存储）将继承应用于该服务器的权限。继承的权限很方便，因为不必手动为 Exchange 组织中的每个对象设置权限。

因为权限的配置和修改方法与 Windows Server 2003 系统的 NTFS 权限设置方法完全一样，所以在此不再赘述，参见本系列的《网管员必读——网络管理》一书。



对 Exchange 对象设置权限时，应使用 Exchange 系统管理器。不要使用 Windows Server 2003 MMC 管理单元（如 Active Directory 站点和服务或 Active Directory 用户和计算机）对 Exchange 对象设置权限。也可以使用 Exchange 委派向导设置权限，并将这些设置应用于整个 Exchange 组织或特定的管理组。由于权限会被继承，因此这些权限控制谁可以查看或谁可以修改服务器级别的设置。在默认情况下，配置这些权限是为了支持标准 Exchange 管理员类型（Exchange 管理员（仅查看）、Exchange 管理员，以及 Exchange 管理员（完全控制））。强烈建议用户使用标准 Exchange 管理员类型，并且只有在组织的安全策略要求更详细的设置的情况下，才应更改这些设置。

10. 全文索引属性设置

单击如图 6-64 所示的对话框中的“全文索引”选项卡，如图 6-65 所示。使用此选项卡可以控制索引期间的服务器性能。

Exchange 可以创建并管理索引，以便加快搜索和查找的速度。早期版本 Exchange 的搜索功能会在每个文件夹中搜索每个项目，因此搜索的时间随着数据库的扩大而增加。使用全文索引，将对数据库中的每个词都编制索引，这样可加快搜索速度。

编制索引是一个非常耗费资源的功能，需要占用大量的 CPU 资源。对于 GB 数量级的数据，编制索引需要数小时或数天的时间。因此，应将编制索引的工作安排在服务器负载不重的情况下进行。

索引是一个非常耗费资源的功能，需要占用大量的 CPU 周期。可以将服务器的使用级别设置为一个较低的值，从而限制索引服务所占用的 CPU 资源。在“系统资源使用情况”下拉列表框中选择以下 4 种系统资源使用值之一：“最低”、“低”、“高”或“最高”。当然具体的选择也不是随意的，一要看使用索引的机会是否多，另外还要考虑到服务器硬件配置和实际应用需求。

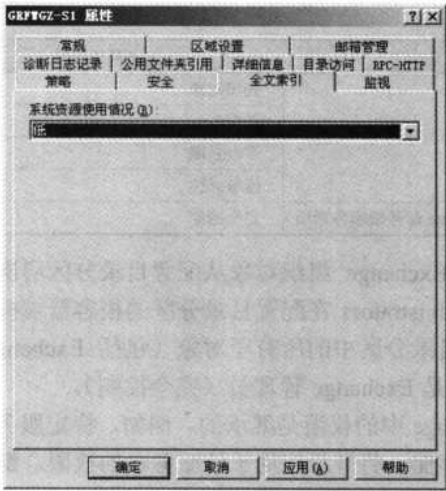


图 6-65 “全文索引”选项卡

11. 监视属性设置

单击如图 6-65 所示的对话框中的“监视”选项卡，如图 6-66 所示。使用此对话框可以选择要在此服务器上监视的资源。可以添加或删除受监视的资源，并设置服务未运行时要向用户显示的错误级别。资源包括 CPU 阈值、可用虚拟内存、可用磁盘空间、SMTP 队列增长、Windows 2000 服务等。

使用此窗口可以查看在此服务器上监视的资源的状态。通过此窗口中的功能，可以查看资源性能的详细信息，并在受监视的资源列表中作更改。双击默认的窗口条目“Microsoft Exchange”服务时，将显示如图 6-67 所示的“默认 Microsoft Exchange 服务”对话框。可以在此对话框中选择要监视的服务。

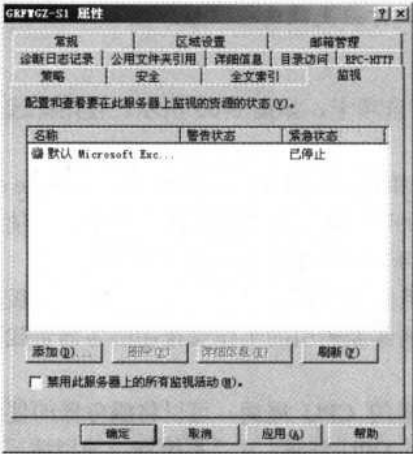


图 6-66 “全文索引”选项卡



图 6-67 “默认 Microsoft Exchange 服务”对话框

单击【添加】按钮，打开如图 6-68 所示的对话框，在此可以选择要监视的服务器资源。

添加的服务将显示在如图 6-66 所示的“监视”选项卡列表中。如果要删除某服务选项，则只需在如图 6-66 所示选项卡资源列表选择相应服务选项后，单击【删除】按钮。单击【详细信息】按钮，在打开的对话框中显示了相应资源的详细信息，可以在各个相应的对话框中查看并更改监视参数。使用【刷新】按钮可以刷新屏幕，这样可以确保监视内容的更改会显示在“监视”选项卡中。

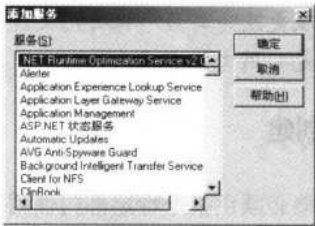


图 6-68 “添加服务”对话框

如果选择了“禁用此服务器上的所有监视活动”复选项，则可以允许或禁止所有服务器监视功能。

6.5 公用文件夹存储和邮箱存储的创建与设置

Exchange 存储使用两种类型的数据库：邮箱存储和公用文件夹存储。邮件服务器系统安装后就会默认各自创建一个，如图 6-69 所示。



图 6-69 系统管理中的邮箱存储和公用文件夹存储

邮箱是发送给指定所有者的所有传入邮件的传递位置。用户邮箱中的信息存储在 Exchange 服务器上的邮箱存储中。邮箱可以包含收到的邮件、邮件附件、文件夹、文档和其他文件。公用文件夹存储是服务器公用文件夹的存储设备。Exchange 支持多个公用文件夹存储。每个公用文件夹存储都包含在一个存储组中。

公用文件夹用于存储可以被组织内所有指定的用户共享的邮件或信息。公用文件夹可以包含不同类型的信息，既可以是简单邮件，也可以是多媒体剪辑和自定义表单。所有公用文件夹及其内容都包含在公用文件夹存储内。邮箱存储与电子邮件系统可以实现从一个用户到多个用户的通信，而公用文件夹则可以实现从多个用户到多个用户的通信。

Exchange 存储数据库（或“存储”）组织成存储组的形式。若使用的是 Exchange Server

2003 标准版，则每个 Exchange 服务器都可以有一个存储组，而每个存储组中包含一个邮箱和一个公用文件夹存储。若使用的是 Exchange Server 2003 企业版，则每个服务器都可以有多达 4 个存储组，其中每个存储组都可以包含多达 5 个数据库（邮箱或公用文件夹存储）。



每个公用文件夹存储与一个公用文件夹树（也称为公用文件夹层次结构）关联。该树必须在创建公用文件夹存储之前已经存在。只能将一个公用文件夹存储从与一棵树关联更改为与另一棵公用文件夹树关联。添加公用文件夹存储时唯一要求的属性是公用文件夹名。

6.5.1 公用文件夹层次结构创建

如果组织内的部分文件与文档必须供某个特定部门使用，则可以创建公用文件夹，以便收集并分发仅与该部门有关的信息。

还可以创建一个新的公用文件夹层次结构（也称公用文件夹树），并指定它自己的数据库。请注意，新建的公用文件夹层次结构被设计成供应用程序访问，而对 Outlook 这样的 MAPI 客户端则不可见。如果希望公用文件夹层次结构对 MAPI 客户端可见，则必须在默认的公用文件夹层次结构的下面创建文件夹。如果只在公用文件夹的下面创建新的文件夹，则不需要配置新的公用文件夹层次结构。可以将所有文件夹配置为接收邮件并支持讨论。

1. 配置新的公用文件夹层次结构

可以在 Exchange 中创建多个公用文件夹层次结构，以便为组织提供更好的安全性和可维护性。例如，可以为公司的人力资源、营销及支持部门创建单独的公用文件夹层次结构，以便提供更高的安全性，并提高对备份和还原的可管理性。

在 Exchange 系统管理器中，每个新建的公用文件夹层次结构都与“公用文件夹”层次结构在同一个层次。每个层次结构都使用其自己的公用文件夹存储。

若要新建公用文件夹层次结构，请执行下列操作。

（1）启动 Exchange 系统管理器，如果已显示管理组，请展开“管理组”节点，再展开相应的组。在相应的管理组下的“文件夹”节点上单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【公用文件夹树】命令，打开如图 6-70 所示的对话框。



图 6-70 “常规”选项卡

(2) 在“名称”文本中键入新公用文件夹树的名称。然后单击【确定】按钮完成公用文件夹层次结构创建。

2. 新建公用文件夹存储

每个公用文件夹层次结构都使用自己的公用文件夹存储。必须先创建层次结构，再创建存储。每个公用文件夹层次结构只能在特定服务器上拥有一个存储。如果每个存储存在不同的服务器上，一个层次结构就可以有多个存储。在这样的配置下，Exchange 会复制存储之间的信息，使层次结构保持一致。

若要创建公用文件夹存储，请执行下列操作。

(1) 在 Exchange 系统管理器中，找到要添加共用文件夹存储的管理组和对应的邮件服务器，在某个特定的存储组上单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【公用存储】命令，打开如图 6-71 所示的对话框。

(2) 在“名称”文本框中键入新数据库的名称，最好与所采用的公用文件夹名称关联。若要将公用文件夹树与数据库关联，单击【浏览】按钮，再选择刚刚创建的公用文件夹层次结构。

(3) 单击【确定】按钮保存设置。此时回到系统管理器界面，即可见到前面创建的公用文件夹和所对应的公用存储，如图 6-72 所示。

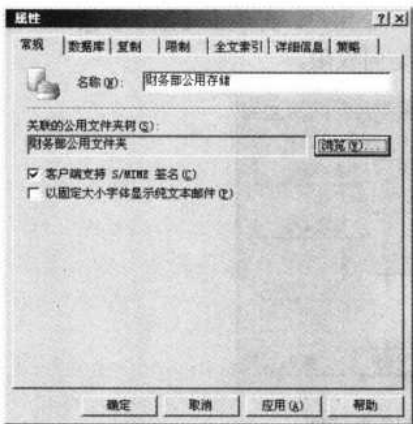


图 6-71 “常规”选项卡

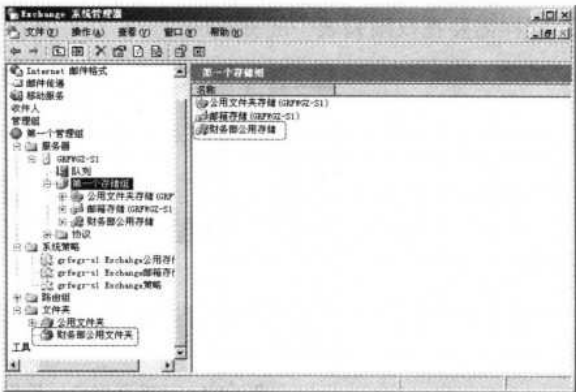


图 6-72 新创建的公用文件夹和公用存储

3. 设置层次结构权限

通过指定哪些用户可以更改层次结构，可以保护公用文件夹层次结构的访问安全性。

(1) 在系统管理器中展开“管理组”，再展开相应的组，找到“文件夹”节点，参见图 6-72。

(2) 在前面创建的公用文件夹中单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“安全”选项卡，如图 6-73 所示。



图 6-73 “安全”选项卡

（3）一般来说除了系统中默认配置的用户权限外，还需要允许相应部门，或者工作组中的用户具有相应公用文件夹树的访问权限。若要修改现有用户，在“组或用户名称”列表中选择用户名，然后在下面的权限列表中重新配置相应的权限。若要授予其他用户访问权，单击【添加】按钮，打开如图 6-74 所示的对话框，选择一个用户，再单击【添加】按钮，然后同样需要在权限列表中配置相应用户对文件夹内容的访问权限。

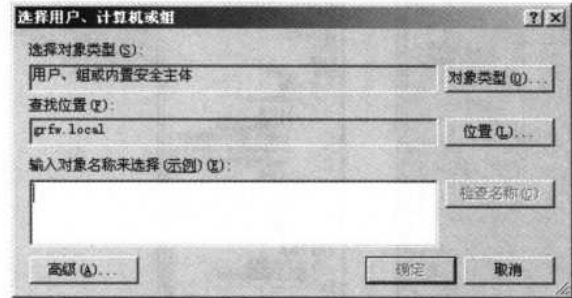


图 6-74 “选择用户、计算机或组”对话框

（4）配置好后在如图 6-73 所示的对话框中单击【确定】按钮完成设置。

4. 查看公用文件夹类型

所有 MAPI 客户端都可以访问默认的公用文件夹树，以读取邮件和存储文档。当创建其他公用文件夹树，以便让应用程序或 Web 浏览器访问时，MAPI 客户端将无法使用该文件夹树。但是，应用程序和 Web 浏览器可以访问默认的公用文件夹树。

若要显示文件夹树类型，只需在如图 6-73 所示的对话框中选择“常规”选项卡，如图 6-75 所示。在“文件夹树的类型”栏中确定哪些客户端可以访问公用文件夹树。



图 6-75 “常规目的”类型公用文件夹树属性对话框“常规”选项卡



注意

如果显示的是“MAPI 客户端”，如图 6-76 所示，那么除应用程序、Web 浏览器及 IFS 共享外，诸如 Outlook 这样的客户端也可以访问该层次结构。如果显示的是“常规目的”，那么该层次结构对于 MAPI 客户端不可见，但应用程序、Web 浏览器及 IFS 共享可以访问该公用文件夹层次结构。



图 6-76 “MAPI 客户端”类型公用文件夹树属性对话框“常规”选项卡

6.5.2 配置新的公用文件夹

一旦创建了公用文件夹层次结构，就可以创建文件夹和子文件夹，来组织提供给用户的内容。具体步骤如下。

- (1) 在如图 6-72 所示的控制台“文件夹”节点中找到要配置复制属性的公用文件夹树（以前面新创建的“财务部公用文件夹树”为例），单击鼠标右键，在弹出的快捷菜单中选择【公用文件夹】命令，打开如图 6-77 所示的对话框。
- (2) 在“名称”文本框中为新建的公用文件夹指定一个象征性的名称。然后单击【确定】按钮完成新的公用文件夹创建。接下来就要为此公用文件夹配置其他属性。
- (3) 在相应公用文件夹树中找到上面新建的公用文件夹，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，然后在打开的对话框中选择“复制”选项卡，如图 6-78 所示。

在此可以将公用文件夹配置为在多个公用文件夹服务器上拥有副本。但在复制配置之前，必须首先在复制的目标服务器上创建公用文件夹存储。应将这些存储与要复制的文件夹所在的层次结构相关联。



图 6-77 “常规”选项卡



图 6-78 “复制”选项卡

若要将文件夹数据库的副本添加到另一台服务器的存储中，单击【添加】按钮，在打开的对话框中配置将文件夹复制到其中的目标服务器，然后单击【确定】按钮。

在“公用文件夹复制间隔”下拉列表框中，选择复制日程安排，或创建一个新的日程安排。若要创建新的日程安排，单击【自定义】按钮，打开如图 6-79 所示的对话框。在“日程安排”窗口中，选择“选定时间”单选项。然后，单击网格上的时间，以指定该文件夹的复制时间。

在“复制邮件优先级”中，设置邮件的优先级。具有紧急发送优先级的邮件将最先传递。

(4) 在如图 6-78 所示的对话框中选择“限制”选项卡，如图 6-80 所示。可以使用“限制”选项卡来控制文件夹的最大大小、设置已删除邮件的保留时间及设置邮件期限。通过对邮件存储限制设置期限和警告，可以节省磁盘空间。在默认情况下，所有设置都采用公用存储的默认设置。取消选中“使用公用存储默认设置”复选项，就可激活下面各设置选项。下面的各个选项说明如表 6-2 所示。

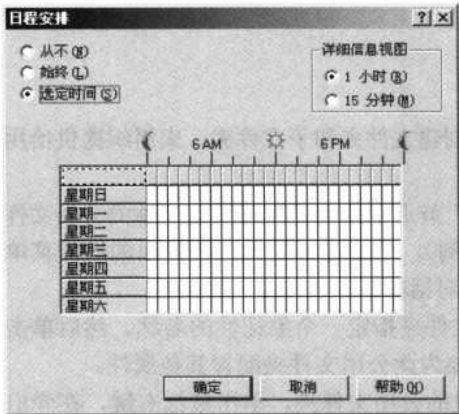


图 6-79 “日程安排”对话框



图 6-80 “限制”选项卡

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

表 6-2 选项说明

限制类型	选项	描述
存储限制	达到该限度时发出警告 (KB)	1~2 097 151 之间的一个数，单位为 KB
	达到该限度时禁止投递 (KB)	1~2 097 151 之间的一个数，单位为 KB
	项目大小最大值 (KB)	1~2 097 151 之间的一个数，单位为 KB
删除设置	保留已删除项目的期限 (天)	1~24 855 之间的一个数，单位为天。在指定的天数之后，所有文件夹内容都将被永久删除
期限	副本期限 (天)	1~24 855 之间的一个数，单位为天。在指定的天数之后，如果此文件夹的副本仍然存在，那么所有这些副本将被永久删除

(5) 在如图 6-80 所示的对话框中选择“限制”选项卡，如图 6-81 所示。权限定义了用户使用文件夹内项目的程度。

在默认情况下，所有用户都有权在公用文件夹内读取或写入内容。可以更改所有用户的权限，或针对特定用户创建不同的权限。若要设置对邮件的访问权，单击【客户端权限】按钮，打开如图 6-82 所示的对话框。

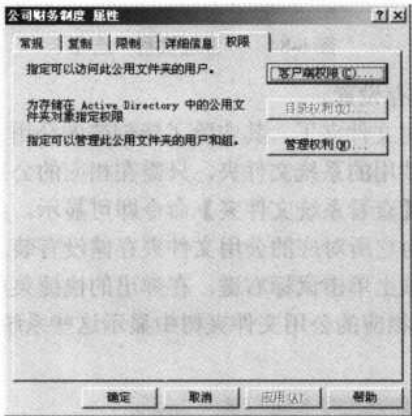


图 6-81 “权限”选项卡

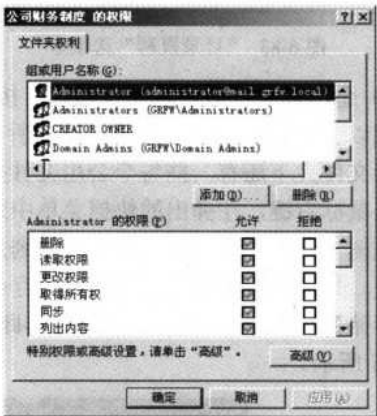


图 6-82 “文件夹权限”选项卡

若要为特定用户创建不同的权限，单击【添加】按钮，打开如图 6-74 所示的对话框。选定一个用户，然后单击【添加】。对要授予权限的所有用户重复此步骤。

在如图 6-81 所示的“权限”选项卡中还可以允许或拒绝对已启用邮件的公用文件夹与电子邮件有关的属性进行更改。Exchange 在 Active Directory 中存储这些属性。若要授予权限，单击【目录权利】按钮（此按钮仅对于已启用邮件的公用文件夹属性对话框中才激活，公用文件的邮件功能启用将在本节后面介绍），打开如图 6-83 所示的对话框，通过单击【添加】按钮，在打开如图 6-74 所示的对话框中添加。在如图 6-83 所示的“权限”列表下，选中“允许”或“拒绝”复选框，以便允许或拒绝每个用户对可用选项进行控制对文件夹的管理员权限。你可以指定哪些用户及组可以使用 Exchange 系统管理器（或自定义管理程序）更改公用文件夹的复制、限制和其他设置。

若要授予管理员对文件夹的权利，单击【管理权利】按钮，打开如图 6-84 所示的对话框。若要访问权授予特定用户，单击【添加】按钮，同样打开如图 6-74 所示的对话框。在其中

选定一个用户，再单击【添加】。对要添加的所有用户重复此步骤。然后在如图 6-84 所示的“权限”列表下，选中“允许”或“拒绝”复选框，以便允许或拒绝每个用户对可用选项的访问。



图 6-83 “目录权利”选项卡



图 6-84 “管理权利”选项卡

(6) 全部设置好后，单击【确定】按钮保存设置。

通过以上设置就可以见到所创建的所有公用文件夹了。其实除了新创建的公用文件夹，每个公用文件夹下还有一些每个公用文件夹都共用的系统文件夹，只需在相应的公用文件夹树上单击鼠标右键，在弹出的快捷菜单中选择【查看系统文件夹】命令即可显示。如果在公用文件夹树下看不到任何系统文件夹，则是因为它所对应的公用文件夹存储没有装入这些公用文件夹。只需在所关联的公用文件夹存储选项上单击鼠标右键，在弹出的快捷菜单中选择【装入存储】命令，然后重启系统管理器即可在相应的公用文件夹树中显示这些系统文件夹，如图 6-85 所示。

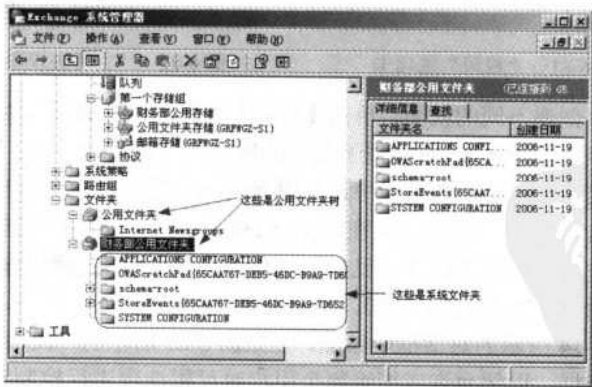


图 6-85 系统管理器中的公用文件夹树和系统文件夹

6.5.3 允许公用文件夹接收邮件

通过对公用文件夹执行启用邮件的操作，并在通信簿中显示该文件夹的名称，可以允许

用户向该文件夹发送邮件，供有权限访问公用文件夹的用户共同查看和使用。



从 Exchange 5.5 迁移的文件夹在默认情况下是已启用邮件的。而对于在纯模式下的 Exchange Server 2003 上创建的文件夹，则必须手动对其进行启用邮件操作。

(1) 在系统管理器中找到要启用邮件功能的相应公用文件夹，单击鼠标右键，在弹出的快捷菜单中选择【启用邮件】命令即可启用相应公用文件夹的邮件功能。

(2) 在启用了邮件功能的公用文件夹上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“常规”选项卡。对比上面给的公用文件夹属性对话框可以看出，启用了邮件功能的公用文件夹属性对话框不仅多了几个与邮件有关的选项卡，而且有些配置选项也发生了改变，对比图 6-77 和图 6-86 可以看出一些改变。

对于创建的每个已启用邮件的公用文件夹，系统都会创建一个通信簿条目。在默认情况下，在使该条目可见并指定显示名之前，文件夹对用户不可见。如果文件夹在通信簿中不可见，只要用户知道该文件夹的地址，并在邮件的“收件人”框中键入该地址，则用户仍然可以向该文件夹投递邮件。但通过在通信簿中显示公用文件夹，可以使所有用户更容易访问它们。

如果希望文件夹在通信簿中的显示名与其在系统管理器中一样，选择“与文件夹名相同”单选项；如果要在通信簿中使用另一个显示名，则选择“使用下列名称”单选项，再键入该文件夹的名称。

(3) 单击“Exchange 高级”选项卡，如图 6-87 所示。如果公用文件夹名包含非 ANSI 字符，可以指定将在通信簿中使用的简单显示名。简单显示名只能使用任何计算机都能读取的字符。在“简单显示名”文本框中可以配置该公用文件夹在 Exchange 地址列表中显示的名称。取消选中“不显示在 Exchange 地址列表中”复选项。即使选择了这一复选项，当用户知道该公用文件夹的名称后同样可以向该公用文件夹中发送邮件。



图 6-86 启用了邮件功能后的公用文件属性对话框“常规”选项卡

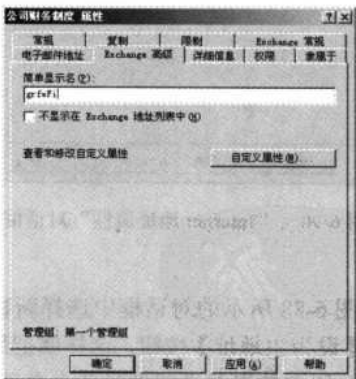


图 6-87 启用了邮件功能后的公用文件属性对话框“Exchange 高级”选项卡

(4) 单击“电子邮件地址”选项卡，如图 6-88 所示。在这个对话框中系统已默认为该公用文件夹配置了两种类型的电子邮件地址。从中可以看出，常用的 SMTP 电子邮件地址太长，可以修改它，以便记忆。当然，也可以新建一个特定的电子邮件地址来代表这个公用文

370 网管员必读——网络应用（第2版）

文件夹的邮件地址，方法是单击【新建】按钮，打开如图 6-89 所示的对话框。在其中选择要新建的电子邮件地址类型，通常为 SMTP。单击【确定】按钮后打开如图 6-90 所示的对话框。在其配置电子邮件地址后，单击【确定】按钮完成新邮件地址的创建。



图 6-88 启用了邮件功能后的公用文件属性对话框“电子邮件地址”选项卡

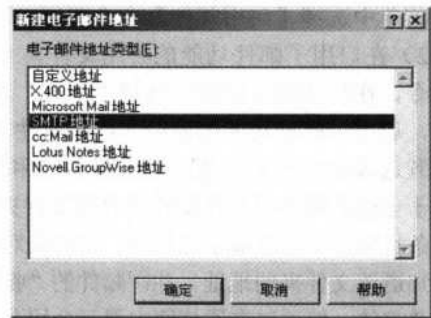


图 6-89 “新建电子邮件地址”对话框

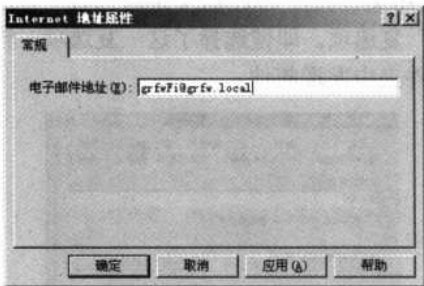


图 6-90 “Internet 地址属性”对话框

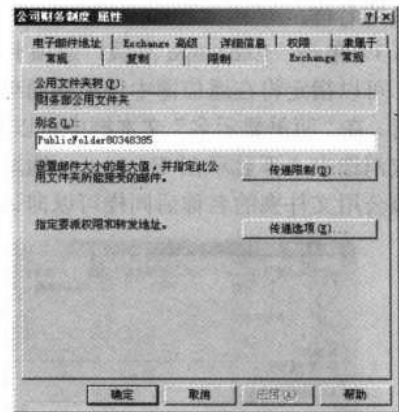


图 6-91 启用了邮件功能后的公用文件属性对话框“Exchange 常规”选项卡

在如图 6-88 所示的对话框中选择新建的电子邮件地址，或者是修改后的原有电子邮件地址，单击【设为主地址】按钮，这样就把新建的邮件地址设为该公用文件夹的默认邮件地址。用户向该公用文件夹发送邮件时就会自动使用这个地址。

(5) 在如图 6-88 所示的对话框中，选择“Exchange 常规”选项卡，如图 6-91 所示。在“别名”文本框中可以为该公用文件夹指定一个别名，用户也可以使用别名向该公用文件夹发送邮件。

单击【传递限制】按钮，打开如图 6-92 所示的对话框。在“发送邮件大小”栏中可以限制所发送的单个邮件大小，选择“最大值 (KB)”单选项，再键入 1~2 097 151 之间的一个数。



图 6-92 “传递限制”对话框

在“接收邮件大小”栏中可限制接收单个邮件的大小，选择“最大值 (KB)”单选项，再键入 1~2 097 151 之间的一个数。

在“邮件限制”栏中，可以创建文件夹将接受其邮件的用户列表。选择“仅来自”单选项，再单击【添加】，打开如图 6-74 所示的对话框。选择一个用户名，再单击【添加】按钮。继续添加，直到要添加的所有用户都已显示出来。选择“来自任何人，除”单选项，可以设置允许接收的用户发来的邮件，单击【添加】按钮，在打开的如图 6-74 所示的对话框中指定允许接收的邮件发件人。继续添加，直到要添加的所有用户都已显示出来。

在如图 6-91 所示的对话框中单击【传递选项】按钮，打开如图 6-93 所示的对话框。在“代表发送”栏中可以设置允许代表公用文件夹发送邮件的用户。若要指定代表公用文件夹发送邮件的用户，则单击【添加】按钮，打开如图 6-74 所示的对话框。选择一个用户，再单击【添加】按钮。继续添加用户，直到要添加的所有用户都出现在下面的方框中，再单击【确定】按钮退出；若要配置邮件发送时的转发地址，则选择“转发到”单选项，再单击【修改】按钮，在打开的如图 6-74 所示的对话框指定可以转发的用户。选中“将邮件传递到转发地址和文件夹”复选项，以便收件人和转发的用户地址这两个位置都可以接收副本。

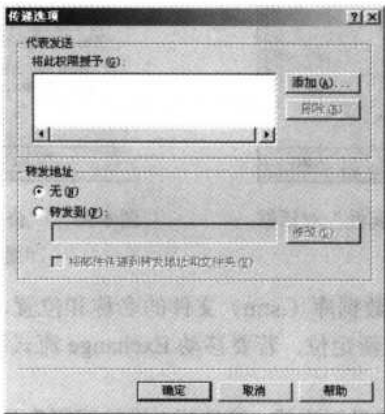


图 6-93 “传递选项”对话框

(6) 设置好后单击【确定】按钮完成公用文件夹邮件功能启用与设置。

6.5.4 公用文件夹存储设置

公用文件夹用于存储可以被组织内所有指定的用户共享的邮件或信息。公用文件夹可以包含不同类型的信息，既可以是简单邮件，也可以是多媒体剪辑和自定义表单。所有公用文件夹及其内容都包含在公用文件夹存储内。邮箱存储与电子邮件系统可以实现从一个用户到多个用户的通信，而公用文件夹则可以实现从多个用户到多个用户的通信。

设置公用文件夹存储属性的方法也是在系统管理器的相应存储组节点下的“公用文件夹存储”子节点上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中进行的。具体配置步骤如下。

(1) 相应存储组节点下的“公用文件夹存储”子节点上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 6-94 所示的对话框。

如果客户端支持 S/MIME，请选择“客户端支持 S/MIME 签名”复选项。禁用该选项可以将具有 S/MIME 签名的邮件转换为不带签名的 MIME 邮件。这样可使无法解释 MIME 的客户端查看带签名的邮件。

若要将可缩放的字体转换为固定大小字体，请选择“以固定大小字体显示纯文本邮件”复选项。

(2) 单击如图 6-94 所示的对话框中的“数据库”选项卡，如图 6-95 所示。若要更改 Exchange 数据库 (.edb) 文件的名称和位置，请单击“Exchange 数据库”项后面的【浏览】按钮重新定位。若要移动 Exchange 数据库，请使用数据库所驻留的服务器上的系统管理器。

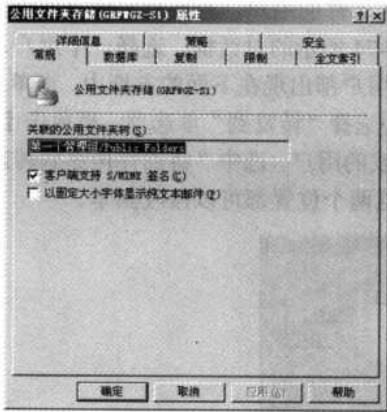


图 6-94 “公用文件夹存储属性”对话框
“常规”选项卡



图 6-95 “公用文件夹存储属性”对话框
“数据库”选项卡

若要更改 Exchange 流式数据库 (.stm) 文件的名称和位置，请单击“Exchange 流式数据库”项后面的【浏览】按钮重新定位。若要移动 Exchange 流式数据库，请使用数据库所驻留的服务器上的系统管理器。

若要生成图形化的自定义日程安排，请选择“维护间隔”下拉列表框中的值，或单击【自定义】按钮，打开如图 6-79 所示的对话框重新维护日程安排。

若要禁止自动装入存储，请选择“启动时不装入此存储”复选项。若要允许数据库覆盖，

请选择“还原时可以覆盖此数据库”复选项。

(3) 单击如图 6-95 所示的对话框中的“复制”选项卡，如图 6-96 所示。若要生成图形化的自定义日程安排，请在“复制间隔”下拉列表框中选择一个值，或单击【自定义】按钮，同样打开如图 6-79 所示的对话框设置复制日程安装。

如果在“复制间隔”下拉列表框中选择的是“始终运行”选项，则可在“‘始终运行’时的复制间隔（分钟）”文本框中键入一个时间值，单位为分钟。若要限制复制邮件的大小，可在“复制邮件大小限制值”文本框中键入一个限制的值，单位为 KB。如果要恢复原来的默认设置，则可直接单击【还原默认设置】按钮即可。

(4) 单击如图 6-96 所示的对话框中的“限制”选项卡，如图 6-97 所示。若要在使用的存储达到指定的值时发出警告，请选择“达到该限度时发出警告（KB）”复选项，然后在后面的文本框中输入一个限制的值，单位为 KB。

若要在使用的存储达到特定的大小时停止发送和接收邮件，请选择“达到该限度时禁止投递（KB）”复选项，然后在后面的文本框中输入一个限制的值，单位为 KB。

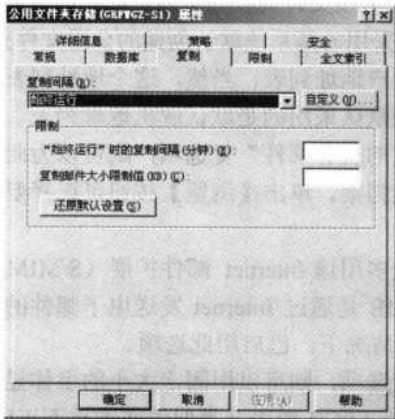


图 6-96 “公用文件夹存储属性”对话框
“复制”选项卡

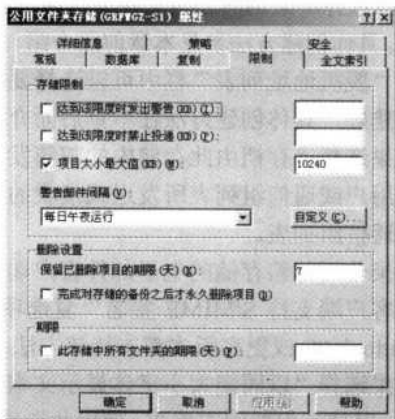


图 6-97 “公用文件夹存储属性”对话框
“限制”选项卡

对于此存储中的公用文件夹，若要限制可以投递或邮寄到其中的项目的大小，请选择“项目大小最大值（KB）”复选项，然后在后面的文本框中输入一个限制的值，单位为 KB。

若要设置警告邮件运行的时间，可在“警告邮件间隔”下拉列表框中选择一个值，或单击【自定义】按钮，打开如图 6-79 所示的对话框进行日程安装。

若要设置已删除项目的保留期，在“保留已删除项目的期限（天）”文本框中设置一个保留的时间，单位为天。若要将项目保留到备份后，选择“完成对存储的备份之后才永久删除项目”复选项。若要设置文件夹中的公用文件的有效期限，选择“此存储中所有文件夹的期限（天）”复选项，然后在后面的文本框中键入一个值，单位为天。



其他几个选项卡的设置与本章 6.4 节介绍的邮件服务器属性对话框中相应选项卡配置方法基本一样，在此不再赘述。

6.5.5 邮箱存储创建与配置

邮箱存储是服务器邮箱的存储设备。Exchange 支持每个服务器中包含多个邮箱存储，每个邮箱存储都包含在一个存储组中。一般来说，邮件服务器系统程序在安装后自动创建一个邮箱存储和公用文件夹存储，但如果认为不够用，想要对用户邮箱存储进行分类，则可另外添加新的邮箱存储，如为单独的部门或人员添加新的邮箱存储，以便与其他用户的邮箱存储区分开来管理。

添加邮箱存储时只需要名称和默认公用文件夹存储两个属性。当然，也可以配置其他更多属性。具体创建与配置步骤如下。

(1) 在系统管理器的相应管理组邮件服务器下的相应存储组上单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【邮箱存储】命令，打开如图 6-98 所示的对话框。在“名称”文本框中可以为新建的邮箱存储指定一个代表性的名称。在“默认公用存储”栏中单击【浏览】按钮可以选择所采用的公用文件夹存储，当然，这个公用文件夹存储必须是已在当前系统中创建了的。具体创建方法参见本章前面介绍。系统默认采用的是系统默认创建的公用文件夹存储。

在“脱机地址列表”栏中可以选择要存储的用户地址列表，当然，这个地址列表也必须事先创建好，具体创建方法在本章后面介绍。系统默认采用的是默认脱机地址列表。

如果选择“存档由此存储中的邮箱发送或接收的所有邮件”复选项，则可以为此邮箱存储中的用户或通信组列表所发送或接收的邮件创建档案。单击【浏览】按钮可选择要存档的邮箱或通信组列表。

如果使用邮箱存储的电子邮件客户端支持安全多用途 Internet 邮件扩展（S/MIME），则选择“客户端支持 S/MIME 签名”复选项。S/MIME 是通过 Internet 发送电子邮件的安全方法，Outlook 98 或更高版本都支持该方法。在默认情况下，已启用此选项。

如果选择“以固定大小字体显示文本邮件”复选项，则可以用固定大小的字体显示纯文本邮件，以使其保持固定格式。使用此选项可以避免 ASCII 图表及类似的文本被不正确显示。

(2) 单击【确定】按钮，完成新建过程。接下来再进行具体配置。

(3) 回到相应存储组上，单击鼠标右键，在弹出的快捷菜单中选择“数据库”选项卡，如图 6-99 所示。

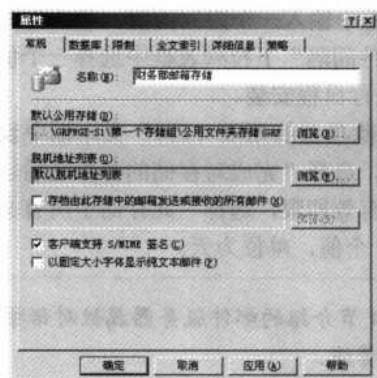


图 6-98 新建邮箱存储属性对话框“常规”选项卡 图 6-99 邮箱存储属性对话框“数据库”选项卡

若要更改 Exchange 数据库（.edb）文件的名称和位置，可在“Exchange 数据库”文本框中直接输入新的数据库文件及所对应的路径，一般无须更改。也可通过单击【浏览】按钮定位。若要更改 Exchange 流式数据库（.stm）文件的名称和位置，则可在“Exchange 流式数据库”文本框中直接输入新的数据库文件及所对应的路径，一般也无须更改。

若要生成图形化的自定义日程安排，可在“维护间隔”下拉列表中选择一个值，或单击【自定义】按钮，在打开的如图 6-79 所示的对话框中设置。

若要禁止自动装入存储，则选择“启动时不装入此存储”复选项；若要允许数据库覆盖，则选择“还原时可以覆盖此数据库”复选项。

(4) 单击“限制”选项卡，如图 6-100 所示。使用“限制”选项卡可以控制用户邮箱的大小，并指定将已删除的项目邮箱中保留多久。还可以指定进行存储限制维护的时间。

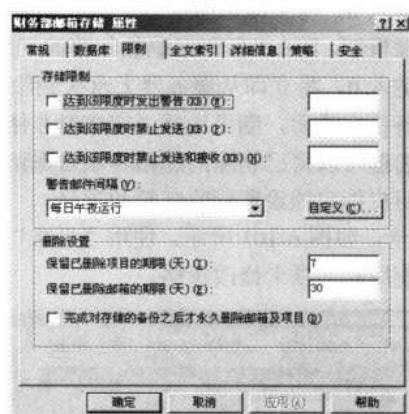


图 6-100 邮箱存储属性对话框“限制”选项卡

使用“存储限制”栏中的选项可以在用户邮箱超过指定的大小限度时向用户发出警告，或禁止他们再发送或接收其他电子邮件。还可以设置一个维护日程安排，以便在通知用户其邮箱已超过指定限度时对邮箱进行维护。

若要在使用的存储达到特定的大小时发出警告，则选择“达到该限度时发出警告（KB）”复选项，然后在后面的文本框中输入一个容量大小的限制值。如果用户的邮箱超过了指定的大小限度，他们将收到电子邮件警告，要求其删除邮箱中的邮件。在默认情况下，此复选框为清除状态。

若要在使用的存储达到特定的大小时停止发送项目，则选择“达到该限度时禁止发送（KB）”复选项，然后在后面的文本框中输入一个容量的限制值。如果用户的邮箱超过了指定的大小限度，他们将收到电子邮件警告，要求其删除邮箱中的邮件。此外，只要邮箱大小尚未降至指定限度以下，用户将无法发送任何电子邮件。在默认情况下，此复选框为清除状态。

若要在使用的存储达到特定的大小时停止发送和接收项目，则选择“达到该限度时禁止发送和接收（KB）”复选项，然后在后面的文本框中输入一个容量大小的限制值。如果用户的邮箱超过了指定大小限度，他们将收到电子邮件警告，要求其删除邮箱中的邮件。此外，只要邮箱大小尚未降至指定限度以下，用户将无法发送任何电子邮件，并且传入的任何邮件都将退回给发件人，同时返回未送达报告（NDR）。

376 网管员必读——网络应用（第2版）

若要生成图形化的自定义日程安排，在“警告邮件间隔”下拉列表框中选择一个值，或单击【自定义】按钮，在打开的如图 6-79 所示的对话框中设置。



注意

此过程非常耗费 CPU 和磁盘空间，因此会降低服务器性能。应在非高峰期安排此类维护。

使用“删除设置”栏中的设置选项可以指定何时将已删除的邮件和邮箱从服务器中永久删除。可以立即或等待指定的天数后删除邮件和邮箱，也可以将已删除的邮件和邮箱一直保留在服务器上，直到执行了备份。

若要设置已删除项目的保留期，则在“保留已删除项目的期限（天）”文本框中输入 0~24 855 之间的一个值。如果键入 0，将立即从服务器上永久删除已删除的项目。

若要设置已删除邮箱的保留期，则在“保留已删除邮箱的期限（天）”文本框中输入 0~24 855 之间的一个值。如果键入 0，将立即从服务器上永久删除已删除的邮箱。

若要将项目一直保留到备份完成后，则可选择“完成对存储的备份之后才永久删除邮箱及项目”复选项。使用此复选框可以将已删除的邮箱和项目保留在服务器上，直到执行了备份。备份完成之后，将根据用户指定的设置删除邮箱和项目。

(5) 单击“策略”选项卡，如图 6-101 所示。使用“策略”选项卡可以检查哪些策略应用于此邮箱存储。用户可以使用此选项卡修改策略。



图 6-101 邮箱存储属性对话框“策略”选项卡

(6) 单击“安全”选项卡，对话框类似如图 6-64 所示。在这里可以配置用户对该邮箱存储文件夹的访问权限。配置方法与图 6-64 所对应的 6.4 节介绍的邮件服务器属性对话框中相应选项卡配置方法基本一样，在此不再赘述。不同的只是所做的设置的作用对象不同。其实也就是 NTFS 访问权限配置，具体参见本系列图书《网管员必读——网络管理》一书。

(7) 全部设置好后单击【确定】按钮完成新邮箱存储的属性设置。

新的邮箱存储新建后，在装入存储邮箱前是空的，只需要在相应邮箱存储上单击鼠标右键，在弹出的快捷菜单中选择【装入存储】命令，即根据在如图 6-98 所示选项卡中配置的地址列表和公用文件夹存储，更新所包含的存储邮箱，如图 6-102 所示。



图 6-102 装入存储后的新邮箱存储

凡是通过 Exchange 邮件服务器发送、接收过的用户、组账户，在“邮箱”文件夹中都会显示一个邮箱，并显示已用的容量，如图 6-103 所示。



图 6-103 “邮箱”文件夹中的用户邮箱

6.6 用户、组邮箱创建与配置

在邮件服务器中，用户和组邮箱的创建与配置是一项基本功能。在 Exchange Server 2003 中，它是与 Windows 服务器系统的 Active Directory 高度集成的，用户邮箱的创建与配置是通过“Active Directory 用户和计算机”管理单元进行的。

6.6.1 已启用邮箱和已启用邮件的收件人的配置

可以使用“Active Directory 用户和计算机”管理单元手动创建收件人，也可以使用 API 通过编程的方法来创建。本节重点讲述如何手动创建已启用邮箱和已启用邮件的对象，包括通信组，这更适合一般用户。

虽然邮件的接收方是人，但是在 Exchange Server 2003 系统中，“收件人”一词指的是 Active Directory 目录服务对象，而不是人。收件人是具有邮件能力的 Active Directory 对象，

378 网管员必读——网络应用（第2版）

但一些 Active Directory 对象，如计算机和打印机就不能作为收件人。但是，对象本身并不接收邮件，邮件也并不存储在 Active Directory 中，它们可以驻留在 Exchange 服务器上的邮箱、公用文件夹或另一个邮件系统中。在 Exchange Server 2003 系统中，以下是默认的已启用邮箱和已启用邮件的收件人。

- 网络用户和组对象。
- 公用文件夹：是已启用邮件的收件人，它与其他收件人有很大的不同。
- InetOrgPerson：只有在具有 Windows Server 2003 域控制器，并且组织中只有 Exchange Server 2003 服务器的情况下，InetOrgPerson 对象才可以是已启用邮件的收件人。

1. “Exchange 常规”选项卡配置

要查看已启用邮箱或者已启用邮件的用户 Exchange 特有选项，只需在“Active Directory 用户和计算机”管理单元上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中查看是否有“Exchange 常规”选项卡，如图 6-104 所示。在这个选项卡中显示了相应用户邮箱所在位置、邮箱别名。还可以对该用户发送邮件的大小和邮箱存储邮件大小进行限制，以及委派权限，配置转发地址。

单击【传递限制】按钮，打开如图 6-105 所示的对话框。使用此对话框可以为已启用邮箱的用户选择传入和传出邮件的大小的最大值，并指定已启用邮箱的用户，或不能接收来自哪些发件人的电子邮件。

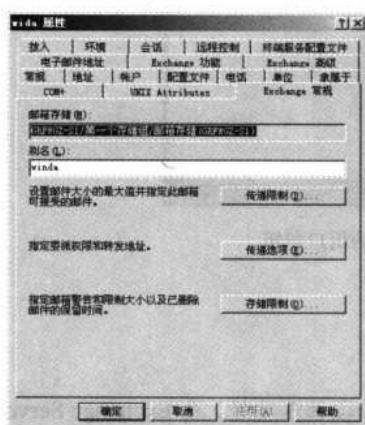


图 6-104 用户属性对话框“Exchange 常规”选项卡

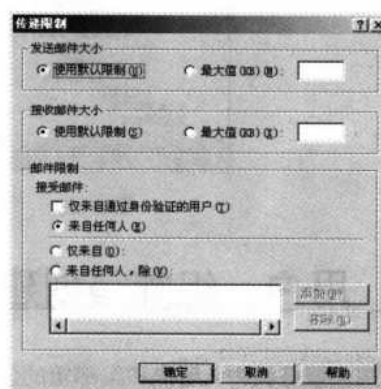


图 6-105 “传递限制”对话框

为了维护系统性能并防止用户由于通过电子邮件基础结构发送大型文件而浪费宝贵的系统资源，应在 Exchange 系统管理器中的全局级别设置邮件大小限制。通常，出于正常业务目的发送的电子邮件应该都不会超过在全局级别设置的阈值（参见图 6-38）。如果某些用户具有特殊要求，并需要发送超出全局限制所允许的大小的文件，可以使用此处的“传递限制”对话框为其覆盖全局设置。

除了设置邮件大小限制外，还可以使用“传递限制”对话框来指定用户可以向哪些人发送邮件，以及可以接收来自哪些人的邮件。这与全局设置中的“发件人筛选”（参见图 6-47）和“收件人筛选”（参见图 6-39）设置类似。

可以通过选中“仅来自通过身份验证的用户”复选项来进一步限制到某收件人的邮件传递。这将阻止任何未通过 Windows 网络身份验证的人向该收件人发送邮件。选中此复选框有效地阻止了发送给该收件人的所有 Internet 邮件。选中此复选框后，可以进一步限制邮件，例如，允许来自每个人（所有已通过身份验证的用户）、仅来自“传递限制”对话框底部的限制列表中的用户或来自除限制列表中的用户以外的每个人的邮件。要将用户添加到限制列表中，通过使用【添加】按钮，在打开的对话框中选择添加。

单击如图 6-104 所示的对话框中的【传递选项】按钮，打开如图 6-106 所示的对话框。使用此对话框可以为已启用邮箱的用户指定邮件传递选项。可以允许一个或多个用户代表已启用邮箱的用户发送邮件，也可以为发送给已启用邮箱的用户的邮件指定一个转发地址，还可以限制已启用邮箱的用户可同时向其发送邮件的收件人数目。

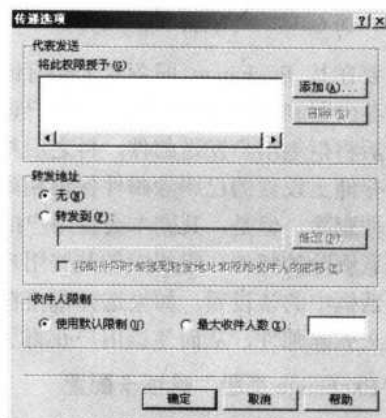


图 6-106 “传递选项”对话框

传递选项之一是使用委派（代表发送）。在许多组织中，都授予被委派者代表另外某人发送邮件的权限。例如，行政助理可以代表经理发送会议请求。可以在“传递选项”对话框中为已启用邮箱的用户指定被委派者。单击【添加】按钮，在打开的对话框中选择添加被委派的用户即可。

另一个传递选项是“转发地址”。在这种情况下，发送给用户的邮件被转发到组织中的另一个地址。还可以选择将邮件的副本同时发送到转发地址和用户的邮箱。在这种情况下，删除邮件的一个副本不会导致另一个副本被删除。可以使用转发来保护实际收件人的身份，或者对帮助其他人整理电子邮件的管理助理使用该选项。

“收件人限制”选项是控制用户在一封邮件中可以包含的收件人数。在默认情况下，不设置限制。

单击如图 6-104 所示的对话框中的【存储限制】按钮，打开如图 6-107 所示的对话框。使用此对话框可以指定邮箱存储限制，当超出此限制时，将向已启用邮箱的用户发出警告，或禁止其发送或接收电子邮件。还可以使用此对话框指定已删除的项目在被永久删除之前在邮箱存储中保留的天数。要重新配置，必须先取消“使用邮箱存储默认设置”复选项的选择。

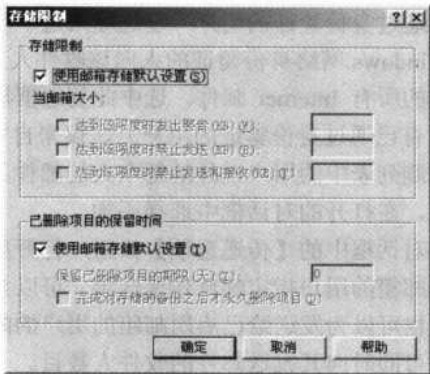


图 6-107 “存储限制”对话框

组织中的个别用户可能需要在其 Exchange 服务器上拥有比邮箱存储所允许的阈值更多的存储空间，此时就可以在“存储限制”对话框中为各个用户设置存储限制。当接近此限制时，可以向用户发出警告，之后将拒绝用户发送邮件，再之后将拒绝用户发送和接收邮件。

此外，还可以覆盖在邮箱存储上设置的已删除邮件保留期限设置。当用户删除某个邮件时，在用户看来似乎已将该邮件删除。但是，其副本会在用户的邮箱存储中保留一段指定的时间，以便可以重新获得被无意删除的邮件。组织中的某些用户可能需要额外的恢复保护，并且可以覆盖“存储限制”对话框中的该设置。如果选择覆盖在邮箱存储上设置的限制，还可以选择对存储备份之前不永久删除邮件，从而使该用户获得更多的恢复机会。

2. “Exchange 功能”和“Exchange 高级”选项卡配置

在如图 6-104 所示的对话框中可以看到，除了“Exchange 常规”这个选项卡外，还有两个与 Exchange 有关的选项卡，那就是“Exchange 功能”和“Exchange 高级”，其对话框分别如图 6-108 和图 6-109 所示。

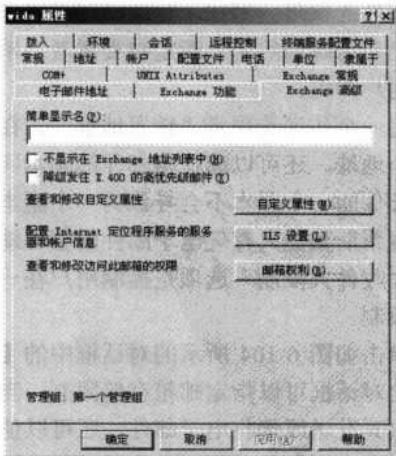


图 6-108 用户属性对话框“Exchange 功能”选项卡 图 6-109 用户属性对话框“Exchange 高级”选项卡

使用“Exchange 功能”选项卡可以为某个用户启用或禁用 Exchange 功能。“Exchange

高级”选项卡应用于已启用邮箱的用户。通过此选项卡，可以选择简单显示名、在地址列表中隐藏已启用邮箱的用户、降级发往 X.400 的高优先级邮件、为自定义属性指定值、选择协议设置及选择 Internet 定位程序服务（ILS）设置。

在“简单显示名”文本框中设置无法解释典型显示名中所有字符的系统将使用的显示名。

当使用多种语言版本的 Exchange 系统管理器来管理 Exchange 组织时，可能会发生这种情形。例如，英文版的 Exchange 系统管理器无法显示日文字符集中的所有字符。由于简单显示名仅采用 ASCII 字符，因此所有版本的 Exchange 系统管理器都能够显示简单显示名。

要防止收件人显示在地址列表中，选择“不显示在 Exchange 地址列表中”复选项；要防止收件人向 X.400 邮件系统发送标记为高优先级的邮件，选择“降级发往 X.400 的高优先级邮件”复选项。

单击如图 6-109 所示选项卡中的【ILS 设置】按钮，打开如图 6-110 所示的对话框。在这里可以指定 Internet 定位程序服务（ILS）服务器和账户名。通过 ILS，Internet 服务提供商和网站管理员可以提高访问网站的用户之间相互通信的能力。ILS 存储与每个用户有关的信息，包括其 IP（Internet 协议）地址，这使联机用户可以相互查找对方。指定此用户的 IIS 设置，一般不用设置。

单击如图 6-109 所示的对话框中的【邮箱权利】按钮，打开如图 6-111 所示的对话框。在这里可以配置网络中各用户和组对象使用该用户邮箱的权限，通常只限制用户本人具有相应权限，其他的都应该删除，包括管理员。通常按系统默认配置即可。在如图 6-111 所示的对话框中的邮件权利如下（其实与 NTFS 文件夹和文件的安全访问权限类似）。

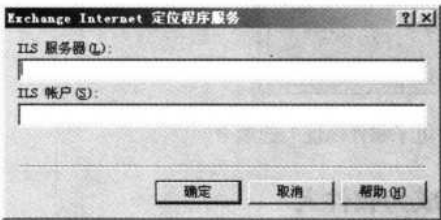


图 6-110 “Exchange Internet 定位程序服务”对话框

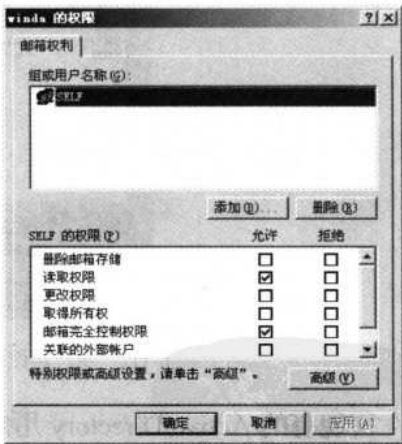


图 6-111 用户邮箱权限对话框

- 删除邮箱存储：可以将该邮箱从邮箱存储中删除。在默认情况下，只有管理员具有执行此项操作的权限。用户无法删除他们自己的邮箱。
- 读取权限：指定的用户可以读取邮箱的内容。
- 更改权限：用户可以修改或删除邮箱中的邮件。
- 取得所有权：用户被授予对邮箱的所有权。
- 邮箱完全控制权限：被委派的用户与所有者具有相同的访问权利。

382 网管员必读——网络应用（第2版）

- 关联的外部账户：当用户的 Windows 账户与 Exchange 邮箱驻留在不同的目录林中时，可以使用该选项。
- 特殊权限：单击【高级】按钮可以对权限进行更精细的处理，包括更改继承。



在如图 6-111 所示的对话框中，一般只需按系统默认选择“SELF”选项即可，无须再加外把用户本身添加进权限列表中，因为 SELF 是一个安全标识符，它代表的就是用户或其他对象本身。“SELF”是 Active Directory 中用户、组或计算机对象上的 ACE（访问控制项）中的占位符。当权限选择 SELF 时，就相当于把权限授予给对象所代表的安全原则。在访问检查期间，操作系统将把 SELF 的 SID 替换为对象所代表的 SID 安全原则。

要查看当前用户的邮箱地址，可在如图 6-109 所示的对话框中选择“电子邮件地址”选项卡，如图 6-112 所示。在这里不仅可以创建新的用户电子邮箱地址（如不同 Exchange 域邮箱地址和互联网邮箱地址等），还可对已有的电子邮箱地址进行修改。如果选择了“基于收件人策略自动更新电子邮件地址”复选项，则用户的可用电子邮件地址会随着收件人策略自动更新。“收件人策略”将在本章后面具体介绍。

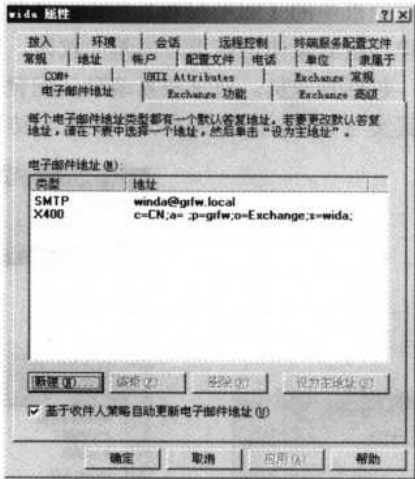


图 6-112 用户属性对话框“电子邮件地址”选项卡

6.6.2 使现有的 Active Directory 用户对象成为收件人

一般情况下，域中的用户都会在安装 Exchange Server 2003 系统会自动成为收件人，具备一个邮箱。如果新建用户对象时没有“创建电子邮件地址”复选项时，则还可以通过以下方法使之成为收件人，其方法如下。

(1) 在“Active Directory 用户和计算机”管理单元的对象上单击鼠标右键，然后在弹出的快捷菜单中选择【Exchange 任务】命令，打开如图 6-113 所示向导对话框。



图 6-113 “欢迎使用 Exchange 任务向导”对话框

(2) 单击【下一步】按钮，打开如图 6-114 所示的对话框。选择“创建邮箱”或“建立电子邮件地址”选项。

注意 如果没有见到“创建邮箱”或“建立电子邮件地址”选项，说明该对象不能成为已启用邮箱的对象。但是，如果列出了“删除邮箱”选项，那么说明该对象已具有与之关联的邮箱。每个收件人都只能有一个 Exchange 邮箱。

(3) 如果在如图 6-114 所示的对话框中选择的是“创建邮箱”选项，单击【下一步】按钮，打开如图 6-115 所示的对话框。在这里可以为该对象配置一个邮箱别名，通常是与用户账户名一样，以便识别。如果在如图 6-114 所示的对话框中选择“建立电子邮件地址”选项，则打开如图 6-116 所示的对话框。在这里除了可以配置邮箱别名和管理组外，还可设置用户的外部电子邮件地址，如关联该用户在其他网络中的邮件地址、互联网地址等。

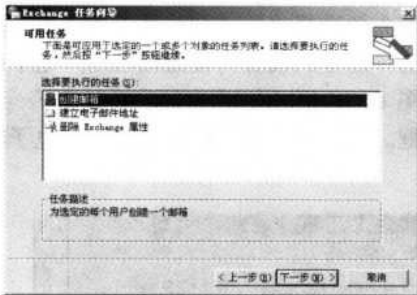


图 6-114 “可用任务”对话框

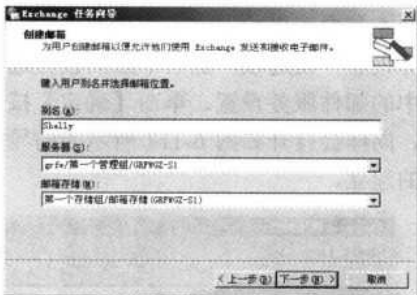


图 6-115 配置邮箱名称和服务器对话框

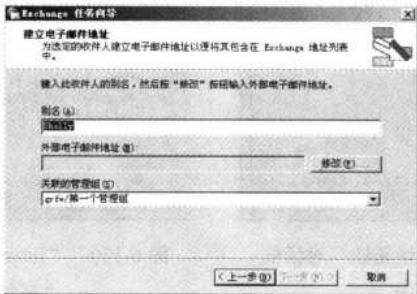


图 6-116 “建立电子邮件地址”对话框

(4) 在如图 6-115 所示的对话框中单击【下一步】按钮，系统会立即为该用户创建邮箱，最终显示如图 6-117 所示的向导完成对话框。

如果要为用户建立电子邮件（其实这里所建立健全的电子邮件地址是用户的外部邮件地址，建立后可以与 Exchange 服务器中的相应用户邮箱账户关联），则在如图 6-116 所示的对话框中配置相关信息，如用户电子邮件账户别名（可任意）和所对应的管理组。至于用户外部电子邮件地址，则需单击【修改】按钮，打开如图 6-118 所示的对话框。在这里要选择外部电子邮件地址（如互联网邮件地址，当然也可以是局域网林中其他域中的邮件服务器类型）的类型，通常为 SMTP 地址类型。



图 6-117 “完成 Exchange 任务向导”对话框

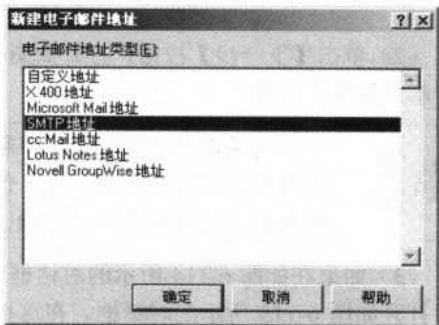


图 6-118 “新建电子邮件地址”对话框

选择电子邮件地址类型，单击【确定】按钮，打开如图 6-119 所示的对话框。在“电子邮件地址”文本框中输入用户对应的外部电子邮件地址即可。选择“高级”选项卡，如图 6-120 所示，在其中可以配置电子邮件地址的邮件格式。首先要选择“覆盖此收件人的 Internet 邮件服务设置”复选项，然后下面的设置选项才被激活。这里的设置将覆盖相应用户电子邮件地址中的邮件服务设置。单击【确定】按钮回到如图 6-116 所示的对话框。单击【下一步】按钮，同样会打开如图 6-117 所示的向导完成对话框。单击【完成】按钮完成用户电子邮件地址的建立。

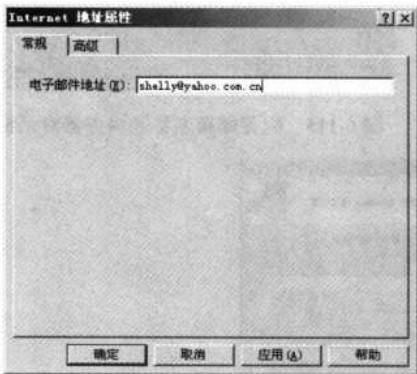


图 6-119 “Internet 地址属性”对话框
“常规”选项卡

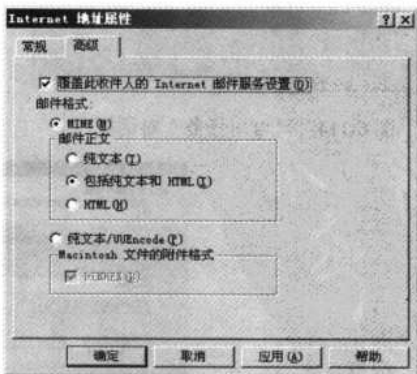


图 6-120 “Internet 地址属性”对话框
“高级”选项卡

6.6.3 为组对象启用邮件

组用于将多个 Active Directory 对象集合到一个名称下，这减少了管理用户，尤其是具有类似需求的用户所需的开销。例如，可能市场组的每个人都必须访问某种网络资源，如公用文件夹。既可以为该组的每个用户授予对该文件夹的访问权限，也可以创建一个名为“marketing”的安全组，并将市场组的每个成员添加到该组中。然后，授予该组对文件夹的访问权限。建立组后，可以授予该组对其他资源（如其他公用文件夹）的访问权限，而不需要每次都找到市场组的每个成员。

主要有两种类型的组：安全组和通信组。安全组是 Active Directory 中的安全主体。这意味着安全组可以在资源（如网络共享或公用文件夹）的访问控制列表（ACL）中设置。通信组的存在是为了便于向用户集合发送电子邮件。在没有 Exchange 的 Windows 环境中，通信组的使用很有限。安全组和通信组都可以是已启用邮件的，但不能是已启用邮箱的，因为它们代表的都是用户集合。

1. 创建已启用邮件的组

已启用邮件的组代表收件人对象集合。其目的是加速邮件分发到多个电子邮件地址的过程。可以像创建其他任何收件人对象一样创建组。

安装了 Exchange 后，在创建组的过程中，会出现如图 6-121 所示的对话框。在其中可以通过选择“创建 Exchange 电子邮件地址”复选项来为组对象创建电子邮件地址。



图 6-121 “新建对象-组”对话框

如果要对现有的组启用邮件，方法与对现有用户对象启用邮件方法一样。

(1) 在相应组上单击鼠标右键，在弹出的快捷菜单中选择【Exchange 任务】命令，首先打开的也是如图 6-113 所示的向导对话框首页。单击【下一步】按钮后，打开如图 6-122 所示的对话框。

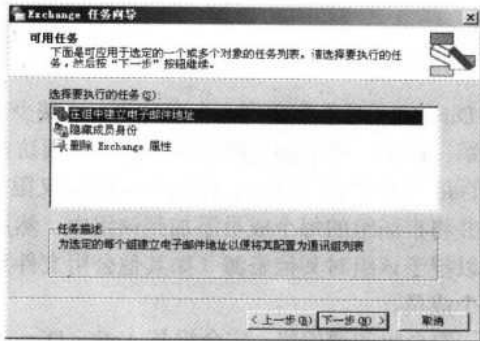


图 6-122 “可用任务”对话框

(2) 选择“在组中建立电子邮件地址”选项，然后单击【下一步】按钮，打开如图 6-123 所示的对话框。在这里要配置组对象的电子邮件地址别名和所关联的管理组。

(3) 单击【下一步】按钮，系统同样会打开一个向导完成对话框，单击【完成】按钮完成组对象电子邮件的启用工作。启用了电子邮件地址的组所对应的电子邮件地址可以在相应组属性对话框“常规”选项卡中查看，如图 6-124 所示。这样下次如果要向组对象中所有用户发送邮件时，就只需向这样一个电子邮件地址中发送，因为组账户对象只能启用电子邮件地址，而不能启用邮箱，所以邮件最终发送到相应组中所有用户邮箱中，都可以查看到该邮件。

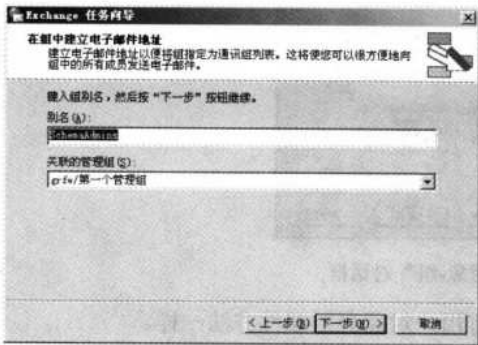


图 6-123 “在组中建立电子邮件地址”对话框

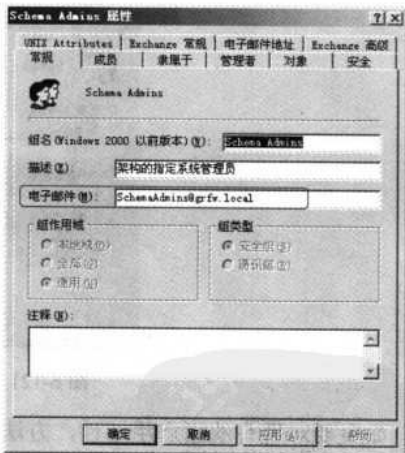


图 6-124 组属性对话框“常规”选项卡

从如图 6-124 所示的属性对话框中可以看出，启用电子邮件地址的组属性对话框中具有用户属性对话框中相关联的 4 个选项卡中的 3 个，即 Exchange 常规、Exchange 高级、电子邮件地址，只是没有“Exchange 功能”选项卡。

2. 展开已启用邮件的组

当邮件发送到某个已启用电子邮件的组时，首先展开组，然后将邮件发送到组中的每一个收件人。除非指定了展开服务器（负责展开通信组的服务器），否则，该组将在处理邮件

的第一台 Exchange 服务器上展开。

大型组的展开会消耗 Exchange 服务器上的大量系统资源。对于大型通信组，可以指定专用的展开服务器，以减轻其他生产服务器的负担。在这种情况下，发往大型通信组的邮件不会使用户用来访问其邮箱的 Exchange 服务器速度减慢。

设置特定服务器作为组的展开服务器存在一个缺点：如果该服务器不可用，通信组的成员将收不到邮件。但是，如果在组属性对话框中“Exchange 高级”选项卡（如图 6-125 所示）的“展开服务器”下拉列表框中保留默认设置“组织中的任意服务器”选项，那么如果某个服务器出现故障，大多数用户仍然可以收到他们的邮件。此外，如果通信组的所有成员都在彼此连接良好的服务器上，那么设置特定的展开服务器也没有必要。

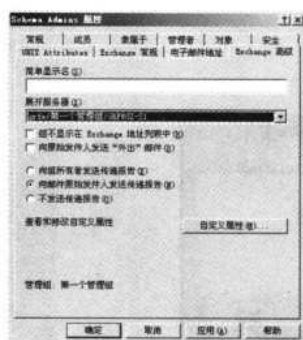


图 6-125 组属性对话框“Exchange 高级”选项卡

3. 在多域环境中使用已启用邮件的组

为了将通信组列表展开为各个收件人，Exchange 会与全局编录服务器联系。全局编录服务器具有它所在域中所有全局组和通用组的副本，以及其他域中通用组的副本，但没有其他域中全局组的副本。这一点在多域环境中很重要，因为如果邮件发往全局编录服务器不属于的域中的某个全局通信组，那么 Exchange 无法展开该邮件中包含的通信组。由于全局编录服务器没有自己所在域之外的域的全局组成员身份的副本，也就不包含有关通信组列表的任何信息。因此，分类程序无法展开通信组列表。为避免此问题，应始终在多域环境中使用通用通信组。应只在单个域中使用全局组。

6.7 策略的创建与管理

Exchange 包括两种策略：系统策略和收件人策略。系统策略是创建并应用于服务器、邮箱存储或公用存储的策略。收件人策略是应用于已启用邮件的 Exchange 对象（至少具有一个电子邮件地址的任何对象）以生成电子邮件地址的策略。

6.7.1 创建服务器策略

使用服务器策略，可以迅速地将常规属性应用于服务器。若要创建服务器策略，必须显示管理组。配置方法参见本章前面介绍。

若要创建服务器策略，执行下列操作。

- （1）启动系统管理器，双击“管理组”节点下要添加策略的管理组。如果还没有系统策略文件夹，必须先创建一个。在相应管理组上单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【系统策略容器】命令即可创建。
- （2）在管理组下找到新建的“系统策略”选项，单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【服务器策略】选项，打开如图 6-126 所示的对话框。
- （3）在“新建策略”对话框中选中要在策略中使用的选项卡所对应的复选框，单击【确定】按钮，打开如图 6-127 所示的对话框。在“常规”选项卡上键入策略名。



图 6-126 新建“服务器策略”时的“新建策略”对话框 图 6-127 新建策略属性对话框“常规”选项卡

- （4）单击“常规（策略）”选项卡，如图 6-128 所示。选择“启用主题日志记录和显示”复选项以记录所有邮件主题字段；选择“启用邮件跟踪”复选项以记录所有 Exchange 组件执行的所有邮件活动；选择“删除日志文件”复选项以删除所有存在时间超过“删除超过以下时间的文件（天）”中设置的值的日志文件。



图 6-128 新建策略属性对话框“常规（策略）”选项卡

6.7.2 创建公用存储策略

使用公用存储策略，可以迅速地将常规、数据库，以及邮件和文件夹限制属性应用于公

用文件夹存储。若要创建服务器策略，也必须显示管理组。

若要创建公用存储策略，执行下列操作。

(1) 在管理组下找到上节新添加的“系统策略”选项，单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【公用存储策略】命令，打开如图 6-129 所示的对话框。在“新建策略”对话框中选中要在策略中使用的选项卡所对应的复选框。此处的选择决定了可以配置的选项卡类型。

(2) 选择好后单击【确定】按钮，打开如图 6-130 所示的对话框。在“常规”选项卡上键入策略名。

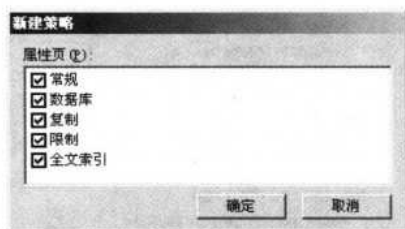


图 6-129 新建“公用存储策略”时的
“新建策略”对话框



图 6-130 公用存储策略属性对话框
“常规”选项卡

(3) 单击“常规（策略）”选项卡，如图 6-131 所示。如果邮件客户端使用的是 S/MIME 标准，请选择“客户端支持 S/MIME 签名”复选项；选择“以固定大小字体显示纯文本邮件”复选项来以固定字体显示变宽邮件字体。

(4) 单击“数据库（策略）”选项卡，如图 6-132 所示。在“维护间隔”下拉列表框中选择用于策略数据库维护的时间间隔的值，或单击【自定义】按钮以图形方式建立自定义维护日程安排。



图 6-131 公用存储策略属性对话框
“常规（策略）”选项卡



图 6-132 公用存储策略属性对话框
“数据库（策略）”选项卡

(5) 单击“复制（策略）”选项卡，如图 6-133 所示。在“复制间隔”下拉列表框中选择一个用来设置复制时间间隔的值，或单击【自定义】按钮以图形方式建立自定义日程安排；在“始终运行”时的复制间隔（分钟）”文本框中键入值以限制复制间隔，然后在“复制邮件大小限制值（KB）”文本框中键入值以限制复制邮件的大小。

(6) 单击“限制（策略）”选项卡，如图 6-134 所示。选择“达到该限度时发出警告（KB）”复选项，在已使用的存储空间达到指定的大小时发出警告；选择“达到该限度时禁止投递（KB）”复选项，禁止发送超过指定大小的邮件；选择“项目大小最大值（KB）”复选项，设置策略中项目的最大限制；在“警告邮件间隔”下拉列表框中选择警告邮件发送的时间间隔值，或单击【自定义】按钮以图形方式建立自定义日程安排。

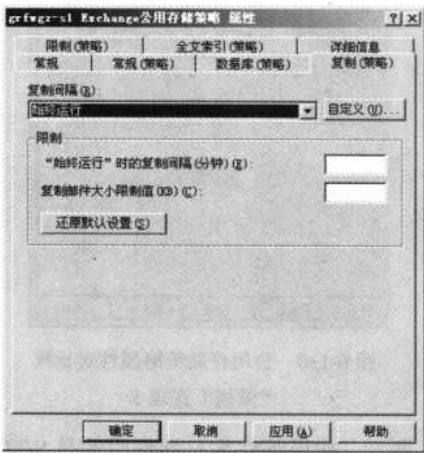


图 6-133 公用存储策略属性对话框
“限制（策略）”选项卡

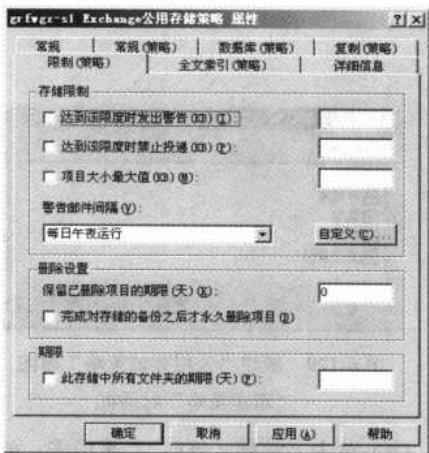


图 6-134 公用存储策略属性对话框
“限制（策略）”选项卡

在“保留已删除项目的期限（天）”选项中可设置已删除项目在存储中保留的最大天数。选择“完成对存储的备份之后才永久删除项目”复选项，则可在备份存储之前保留其中的项目。在“此存储中所有文件夹的期限（天）”文本框中可以键入限制所有文件夹在此存储中的保留时间（天数）。

6.7.3 创建邮箱存储策略

使用邮箱存储策略，可以迅速地将常规、数据库和邮件限制属性应用于邮箱存储。若要创建服务器策略，也必须显示管理组。

若要创建邮箱存储策略，执行下列操作。

(1) 在“管理组”节点找到 6.7.1 节新建的“系统策略”，单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【邮箱存储策略】命令，打开如图 6-135 所示的对话框。此处的选择也决定了可以配置的邮箱存储属性选项类型。

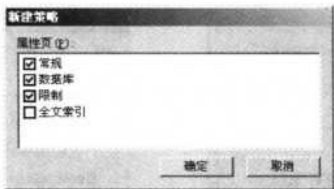


图 6-135 新建邮箱存储时的“新建策略”对话框

(2) 在“新建策略”对话框中选中要在策略中使用的选项卡所对应的复选框。然后单击【确定】按钮，打开如图 6-136 所示的对话框。在“常规”选项卡上键入策略名。

(3) 单击“常规（策略）”选项卡，如图 6-137 所示。在“默认公用存储”中通过单击【浏览】按钮打开对话框设置默认的公用存储位置。在“脱机地址列表”中同样可通过单击【浏览】按钮，在打开的对话框中设置脱机地址列表。如果邮件客户端使用的是安全/多用途 Internet 邮件扩展 (S/MIME) 标准，请选择“客户端支持 S/MIME 签名”复选项；选择“以固定大小字体显示纯文本邮件”复选项以固定字体显示变宽邮件文字。



图 6-136 邮箱存储策略属性对话框
“常规”选项卡

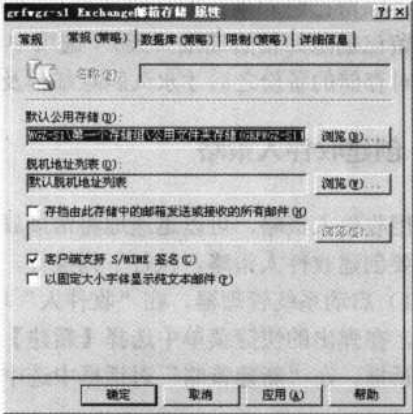


图 6-137 邮箱存储策略属性对话框
“常规（策略）”选项卡

(4) 单击“数据库（策略）”选项卡，如图 6-138 所示。在“维护间隔”下拉列表框中选择一个用于策略数据库维护的时间值，或单击【自定义】按钮以图形方式建立自定义数据库维护日程安排。

(5) 单击“限制（策略）”选项卡，如图 6-139 所示。选择“达到该限度时发出警告 (KB)”复选项，在已使用的存储空间达到指定的大小时发出警告；选择“达到该限度时禁止发送 (KB)”复选项，在已使用的存储空间达到指定的大小时停止发送邮件；选择“达到该限度时禁止发送和接收 (KB)”复选项，在已使用的存储空间达到指定的大小时停止发送和接收邮件；在“警告邮件间隔”下拉列表框中选择一个警告邮件发送地时间值，或单击【自定义】按钮以图形方式建立自定义警告邮件发送日程安排。



图 6-138 邮箱存储策略属性对话框
“数据库（策略）”选项卡

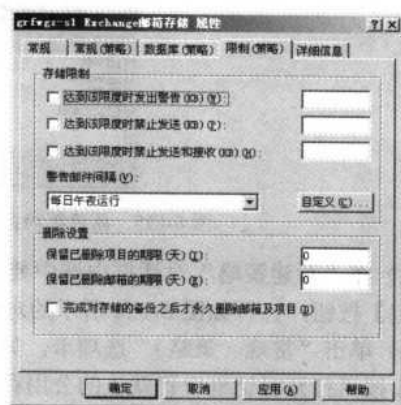


图 6-139 邮箱存储策略属性对话框
“限制（策略）”选项卡

在“保留已删除项目的期限（天）”选项中设置已删除项目在存储中保留的最大天数。在“保留已删除邮箱的期限（天）”选项中设置已删除邮箱在存储中保留的最大天数。选择“完成对存储的备份之后才永久删除邮箱及项目”复选项，在备份存储之前保留邮箱和项目。

6.7.4 创建收件人策略

使用收件人策略，可以迅速地常规属性和电子邮件地址属性应用于收件人。若要创建收件人策略，执行下列操作。

（1）启动系统管理器，在“收件人”项的“收件人策略”（如图 6-140 所示）上单击鼠标右键，在弹出的快捷菜单中选择【新建】项下的【收件人策略】命令，打开如图 6-141 所示的对话框。在“新建策略”对话框中选中要在策略中使用的选项卡所对应的复选框。



图 6-140 “Exchange 系统管理器”控制
“收件人策略”选项

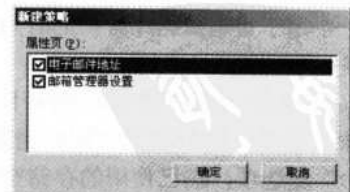


图 6-141 新建收件人策略时的
“新建策略”对话框

（2）单击【确定】按钮，打开如图 6-142 所示的对话框。在“常规”选项卡上的“名称”文本框中输入收件人策略的名称。



图 6-142 收件人策略属性对话框“常规”选项卡

(3) 单击【修改】按钮，打开如图 6-143 所示的对话框。在其中选择适用该策略的收件人。使用“常规”选项卡可以建立简单查询；使用“存储”选项卡可以指定查询中要包括的邮箱组；使用“高级”选项卡可以建立使用收件人的字段级属性和搜索条件的高级查询。

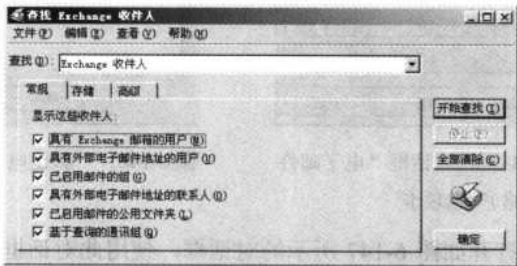


图 6-143 “查找 Exchange 收件人”对话框

(4) 配置好后，可以单击【开始查找】按钮，将在对话框中显示所设置的适用于该收件人策略的用户，或组账户，如图 6-144 所示。



图 6-144 显示收件人后的“查找 Exchange 收件人”窗口

394 网管员必读——网络应用（第2版）

(5) 在如图 6-142 所示的对话框中选择“电子邮件地址（策略）”选项卡，如图 6-145 所示。选择“生成规则”列表，查看为 LDAP 查询所选定的收件人生成电子邮件地址的当前规则。此策略下的任何收件人将自动拥有此列表中的地址。

(6) 单击【新建】按钮，打开如图 6-146 所示的对话框。在这里可以添加新的邮件地址规则（也就是邮件地址格式）。选择一种电子邮件地址类型后，在此以选择 SMTP 邮件地址类型为例进行介绍。



图 6-145 收件人策略属性对话框“电子邮件地址（策略）”选项卡

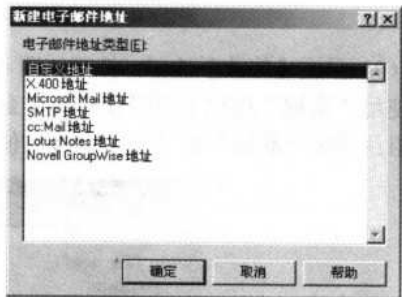


图 6-146 “新建电子邮件地址”对话框

单击【确定】按钮打开如图 6-147 所示的对话框，使用此对话框可以创建和修改 SMTP 电子邮件地址。在“地址”文本框中输入新的 SMTP 电子邮件地址，然后单击【确定】按钮返回到如图 6-145 所示的对话框中。这样新添加的电子邮件地址都将同时显示在如图 6-144 所示的“搜索结果”列表中。作为它们共同的电子邮件地址。在如图 6-145 所示的对话框中，使用【编辑】按钮可以更改现有规则。



图 6-147 “SMTP 地址属性”对话框“常规”选项卡

存在两个或多个地址类型相同的电子邮件地址时，选择一个主要邮件地址后，在如图 6-145 所示的对话框中单击【设为主地址】按钮将它指定为主地址。

(7) 在如图 6-145 所示的对话框中选择“邮箱管理器设置（策略）”选项卡，如图 6-148 所示。用此选项卡可以配置邮箱管理器收件人策略。请选择要处理的邮箱文件夹，并指定要对超出策略限制的邮件采取的操作。



图 6-148 收件人策略属性对话框“邮箱管理器设置（策略）”选项卡

在“当处理邮箱时”下拉列表框中可以选择要对超出策略限制的邮件采取的操作。在“处理每个文件夹中超过指定大小和期限的邮件”列表中可以选处理哪些文件夹。若要设置期限和大小限制，请单击该文件夹，再单击【编辑】按钮。邮箱管理器会检查所选文件夹中是否存在超过策略限制的邮件。



注意

配置日历项处理设置时请考虑下列事项：如果选中“期限（天）”复选项，并将值配置为“0”，将不会处理将来的任何约会；如果清除“期限（天）”复选项，并单击【确定】按钮，将会处理所有的日历项，包括将来的项目（但不包括定期项目）。单击【确定】按钮之后，“邮箱管理器设置（策略）”上的“期限（天）”列将设置为“任意”；如果选中“期限（天）”复选项，并将值配置为 X，则所有超过 X 天的日历项都将得到处理。此外，所有当前及将来的日历项在达到 X 天后也将得到处理。

选择“处理之后向用户发送通知邮件”复选项，可以在邮箱处理完毕后向用户发送电子邮件通知。若要自定义邮件，请选中此复选框并单击【邮件】按钮。选择“排除特定的邮件类别”复选项，并单击【自定义】按钮可以将某些邮件类别排除在删除操作外。



注意

如果选择了默认文件夹（默认情况下包含除邮件及投递项目之外的项目类型），则默认项目类型与该类型匹配的所有文件夹都将得到处理。例如，如果选择“便笺”文件夹（默认情况下包含便笺项目），且相应的邮箱有一个默认项目类型为“便笺”的用户创建文件夹，则该用户创建文件夹也将得到处理。

创建好收件人策略后如果要立即应用此策略，则需在如图 6-148 所示的对话框中选择相应的策略，单击鼠标右键，在弹出的快捷菜单中选择【立即应用此策略】命令即可。



注意

创建新的邮箱收件人策略时，收件人更新服务会为成员邮箱分配唯一的ID。此ID将邮箱与策略相关联，因此邮箱管理器能够知道应对指定的邮箱应用哪个邮箱收件人策略。如果修改邮箱收件人策略而使成员身份被修改，【立即应用此策略】命令会立即将新的邮箱与该策略相关联，而无须等待运行收件人更新服务。但是，此命令不会影响以前是该策略的成员但现在不再是成员的邮箱。这些邮箱将继续受到邮箱管理器的影响，直到收件人更新服务下次运行并将这些邮箱从策略中删除。收件人更新服务自动运行，因此成员身份始终会得到更新，但是，管理员应该意识到，根据收件人更新服务更新策略信息所花费的时间，邮箱管理器可能会临时处理不再包括在邮箱收件人策略中的邮箱。

6.7.5 将系统策略应用于对象

上节介绍了应用收件人策略的方法，它的方法比较简单，直接选择右键菜单中的【立即应用策略】命令即可。在系统策略中的应用配置相对比较复杂一些，它需要在策略中添加同一类型的 Exchange 对象。

若要将策略应用于对象，请执行下列操作。

(1) 在启动系统管理器的组织或管理组项下，选择“系统策略”选项。在详细信息窗口中要修改的策略上单击鼠标右键，在弹出的快捷菜单中选择对应的添加选项（如果该策略原来就是“公用存储策略”，则快捷菜单中出现的就是【添加公用存储】命令；如果原策略是“邮箱存储策略”，则在快捷菜单中出现的就是【添加邮箱存储】命令，依次类推）。选择相应选项后，打开如图 6-149 所示的对话框。在其中可以选择要应用该策略的新对象（一定要是对应策略所作用的对象类型，如此处添加的邮箱存储，就必须是服务器中已在存的“邮箱存储”；如果添加的是公用文件夹存储，则一定要是服务器上已存在“公用文件夹存储”对象，依次类推），如果要同时添加多个对象，可用分号（;）隔开。

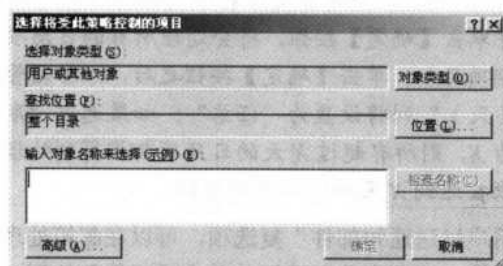


图 6-149 “选择将受此策略控制的项目”对话框

(2) 全部添加好后，单击【确定】按钮，弹出一个“Microsoft Exchange Administrator”提示框，此对话框提示确认是否要将对象添加到策略。单击【是 (Y)】按钮添加。

如果所添加的对象已受另一个策略的控制，将显示另一个“Microsoft Exchange Administrator”提示框，提示验证是否要使对象不受另一个策略的控制。确认后单击【是 (Y)】按钮，使添加的对象脱离原策略的控制。

(3) 添加好后，要立即应用该系统策略，则可在系统管理器控制台相应管理组下的“系

统策略”选项中的相应策略项上单击鼠标右键，在弹出的快捷菜单中选择【立即应用】命令。

6.8 SMTP 协议配置

在 Exchange 中，使用 SMTP 虚拟服务器和 SMTP 连接器控制 SMTP 的配置。SMTP 虚拟服务器本质上是一个 SMTP 堆栈（既接收电子邮件，也充当发送电子邮件的客户端的进程或服务）。每个 SMTP 虚拟服务器都代表服务器上的一个 SMTP 服务实例。因此，一个物理服务器可以驻留多个虚拟服务器。

SMTP 虚拟服务器由 IP 地址和端口号的唯一组合定义。IP 地址是 SMTP 虚拟服务器用来侦听传入 SMTP 的连接地址。默认的 IP 地址是“所有未分配”，但这并不意味着该 SMTP 虚拟服务器没地址可用，而是意味着 SMTP 虚拟服务器在任意可用的 IP 地址上执行侦听。端口号是 SMTP 虚拟服务器用来接收通信的端口。到 SMTP 虚拟服务器的入站连接的默认端口号是端口 25。

使用 Exchange 系统管理器可以控制大多数 SMTP 设置。SMTP 虚拟服务器的属性设置控制着入站邮件及出站邮件设置（程度较低）。

SMTP 连接器用于指定邮件的独立路由。可以使用 SMTP 连接器建立 Internet 邮件的网关，或者连接到特定的域或邮件系统。连接器可以为指定的邮件路由指定具体的选项。

虽然可以使用 SMTP 虚拟服务器发送或接收 Internet 邮件，但大多数公司都配置 SMTP 连接器来路由 Internet 邮件。使用 SMTP 连接器是推荐选项，因为它为发送到 Internet 的邮件提供独立的路由。此外，SMTP 连接器上的可用配置选项数大于 SMTP 虚拟服务器上的可用配置选项数。以下各节描述了使用 Internet 邮件向导及手动配置 Exchange 以发送 Internet 邮件的过程，包括有关创建和配置 SMTP 连接器以路由 Internet 邮件的信息。

6.8.1 使用向导配置 Internet 邮件

Exchange Server 2003 实现了新版本的 Internet 邮件向导，该向导可以帮助用户配置与 Exchange Server 2003 或 Exchange 2000 Server 的 Internet 邮件连接。使用 Internet 邮件向导，可以配置 Exchange 服务器以发送 Internet 邮件、接收 Internet 邮件或发送并接收 Internet 邮件。此外，使用 Internet 邮件向导意味着不必手动配置 SMTP 连接器和 SMTP 虚拟服务器。Internet 邮件向导自动创建传出 Internet 邮件所必需的 SMTP 连接器，并配置 SMTP 虚拟服务器以接受传入邮件。



如果已设置了 SMTP 连接器、修改了默认 SMTP 服务器的 IP 地址或端口号，或者在 Exchange 服务器上创建其他 SMTP 虚拟服务器，将无法运行 Internet 邮件向导。但是，如果将服务器的配置重置为其默认状态，则可以运行 Internet 邮件向导。另外，Internet 邮件向导主要用于环境复杂性低于大型企业公司的中小型公司。若用户具有复杂的或企业邮件传递环境，必须手动配置 Exchange 以传递 Internet 邮件。

启动 Internet 邮件向导的步骤如下。

(1) 在 Exchange 系统管理器的 Exchange 组织节点（本示例为 grfw（Exchange））上单击鼠标右键，在弹出的快捷菜单中选择【Internet 邮件向导】命令，打开如图 6-150 所示的对话框。

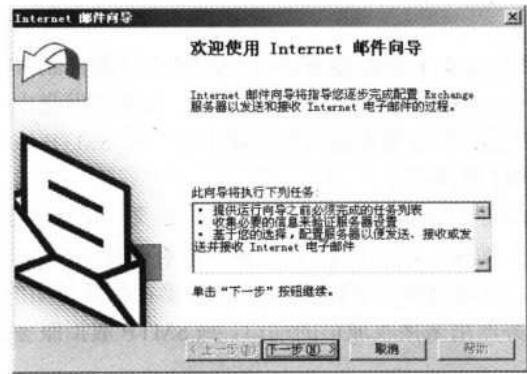


图 6-150 “欢迎使用 Internet 邮件向导”对话框

(2) 单击【下一步】按钮，打开如图 6-151 所示的对话框。在这里提示了要进行向导所必须具备的一些基本条件，检查当前邮件服务器是否具有所列条件。

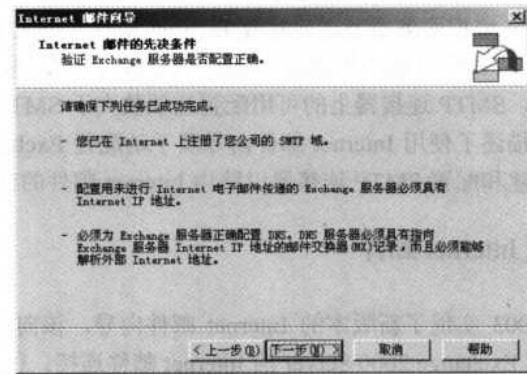


图 6-151 “Internet 邮件的先决条件”对话框

(3) 单击【下一步】按钮，打开如图 6-152 所示的对话框。在这里要选择运行向导的邮件服务器。要注意“在以下情况下不能运行此向导”列表中所列出的例外。其中包括不允许是 Exchange 5.5 或更早期版本的邮件服务器，也不能是网络群集中的一部分。

(4) 单击【下一步】按钮，系统开始测试用户所选的邮件服务器是否满足所列的条件，如果通过测试，则打开如图 6-153 所示的对话框，可以继续向下进行向导了。否则就只能退出向导，重新配置服务器，使它满足所列的基本条件（包括如图 6-151 和图 6-152 所示的对话框中列出的条件）。



图 6-152 “选择服务器”对话框

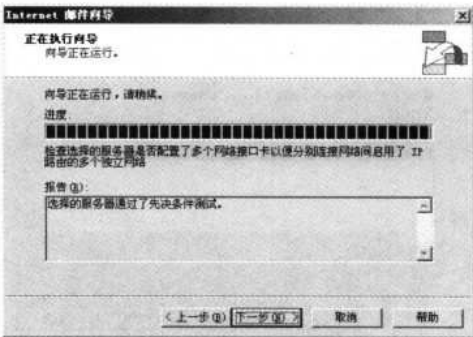


图 6-153 “正在执行向导”对话框

(5) 单击【下一步】按钮，打开如图 6-154 所示的对话框。在这里要选择该邮件服务器所应具备的 Internet 邮件功能，可以只是作为 Internet 邮件发送服务器，选择“发送 Internet 电子邮件”复选项，发送邮件服务器中用户的 Internet 电子邮件；也可以只是作为 Internet 邮件接收服务器，选择“接收 Internet 电子邮件”复选项，接收服务器中用户的 Internet 邮件。当然也可以同时担当这两种功能，只需同时选择两个复选项即可，在此以同时选择为例。

(6) 单击【下一步】按钮，打开如图 6-155 所示的对话框。在此要选择入站邮件的 SMTP 域，还可以新建 SMTP 域，但如果在邮件服务器上创建了除“默认策略”以外的其他收件人策略，则不能在对话框中新建 SMTP 域。

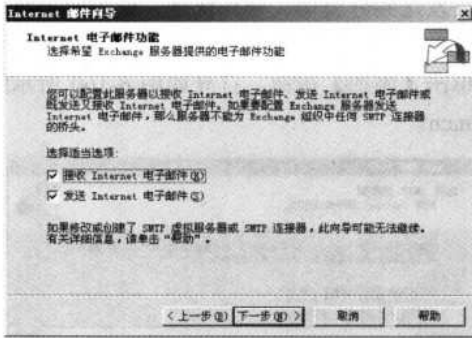


图 6-154 “Internet 电子邮件功能”对话框

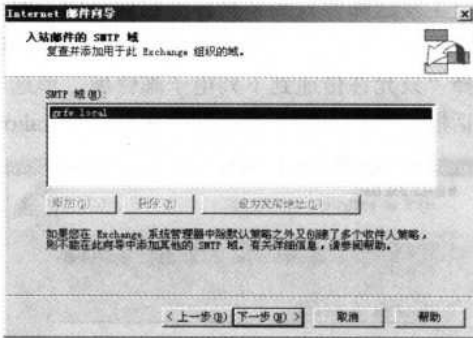


图 6-155 “入站邮件的 SMTP 域”对话框

(7) 单击【下一步】按钮，打开如图 6-156 所示的对话框。在这里要选择出站邮件的 SMTP 虚拟服务器，用做桥头服务器，起到内、外部邮件服务器的桥接作用。对于只有一台 Exchange 邮件服务器的中小型企业，则上一步所选的入站 SMTP 域和本步所选的出站桥头服务器都是同一台服务器。

(8) 单击【下一步】按钮，打开如图 6-157 所示的对话框。在这里要选择出站邮件发送到 Internet 邮件服务器所使用的方式。可以使用 DNS 域名解析方式，也可以使用路由方式。如果企业网络中有企业路由器（也可以是提供 DNS 中继功能的宽带路由器），或者配置了路由服务的主机，则可选择“通过下列智能主机路由所有邮件”单选项，然后在下面的文本框中输入路由器的 IP 地址，也可以输入主机名。如果是 IP 地址，则一定要用[]括起整个 IP 地址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

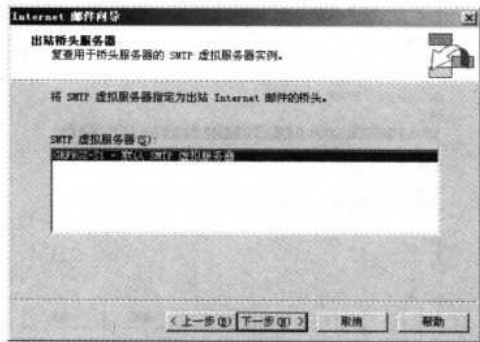


图 6-156 “出站桥头服务器”对话框

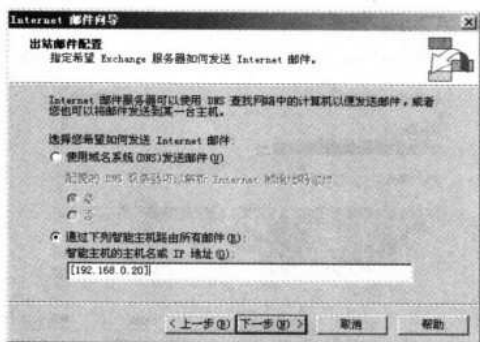


图 6-157 “出站邮件配置”对话框

如果没有路由器，而配置了 DNS，则可选择“使用域名系统（DNS）发送邮件”单选项，然后在“配置的 DNS 服务器可以解析 Internet 域地址吗？”栏中选择所配置的 DNS 服务器是否具有 Internet 域名解析功能，如果有则选择“是”单选项。通常的企业内部 DNS 不具备这个功能，所以选择“否”单选项，此时单击【下一步】按钮时会打开如图 6-158 所示的对话框，要求指定一个具有 Internet 域名解析功能的外部 DNS 服务器（通过单击【添加】按钮添加即可）。

(9) 单击如图 6-157 或者图 6-158 所示的对话框的【下一步】按钮，均可打开如图 6-159 所示的对话框。在这里要选择出站 SMTP 服务器所发送的电子邮件所对应的邮件域，可以限制员工发送邮件只到某些外部邮件域中，如只允许发送到分公司、合作伙伴、供应商等单位员工所统一使用的邮件域，如统一为 163 邮箱，或者某企业的外部邮件服务器域。此时需要选择“只允许传递到下列电子邮件域”单选项，单击【添加】按钮，打开如图 6-160 所示的对话框，在其中输入对应邮件域名，如 yahoo.com.cn。

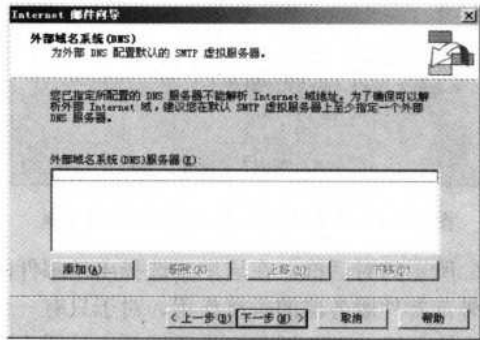


图 6-158 “外部域名系统（DNS）”对话框

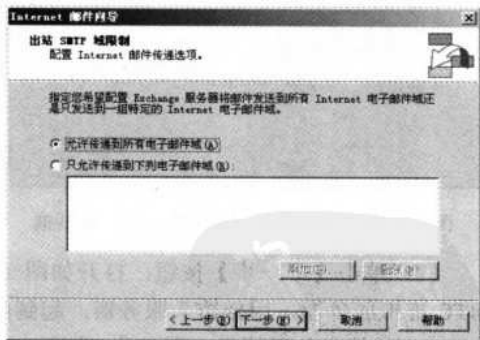


图 6-159 “出站 SMTP 域限制”对话框

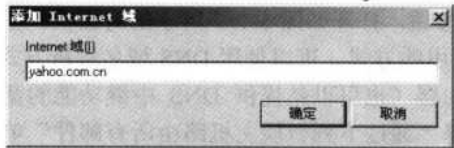


图 6-160 “添加 Internet 域”对话框

如果允许员工向任何邮件域（其实就是任何人）发送外部邮件，则可选择“允许传递到所有电子邮件域”单选项。

(10) 单击【下一步】按钮，打开如图 6-161 所示的对话框。在这里显示的是以上配置的摘要，可以一一查看，发现不妥之处，可以通过单击【上一步】按钮返回到相应步骤重新配置。确认无误后可直接单击【下一步】按钮，打开如图 6-162 所示向导完成对话框。单击【完成】按钮完成“Internet 邮件向导”。如果要在关闭向导时查看详细的配置报告，可以选择如图 6-162 所示的对话框中的“关闭向导时查看详细报告”复选项，这样在单击【完成】按钮时会打开一个详细的配置向导，一方面可供进一步核对，另一方面也可方便日后查阅相关配置。

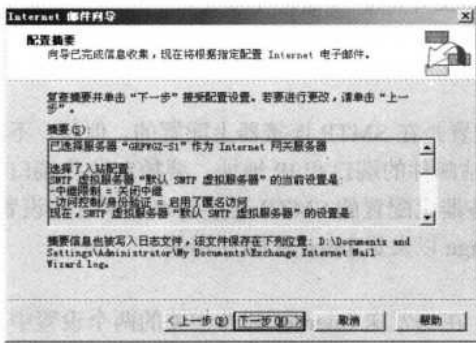


图 6-161 “Internet 邮件向导”对话框



图 6-162 “正在完成 Internet 邮件向导”对话框

6.8.2 使用向导配置双宿主服务器

使用 Internet 邮件向导在双宿主服务器（这样的服务器配置了两个或多个网络地址，并且通常有两个网卡）上配置 Internet 邮件传递时，向导除了将执行上节所介绍的必要配置步骤外，还会在 Exchange 服务器上创建其他 SMTP 虚拟服务器。它以下列方式配置 Internet 邮件传递。

- 要配置服务器以发送 Internet 邮件，向导将引导你完成成为默认 SMTP 虚拟服务器（将在其上创建 SMTP 连接器以发送出站邮件）分配 Intranet IP 地址的过程。为该虚拟服务器分配 Intranet IP 地址，以便只有在你的 Intranet 内部用户才能发送出站邮件。
- 配置服务器以接收 Internet 邮件，向导将引导你完成成为 Internet SMTP 虚拟服务器分配 Internet IP 地址的过程。之所以要为该虚拟服务器分配 Internet IP 地址，是因为外部服务器必须能够连接到该 SMTP 虚拟服务器才能发送 Internet 邮件。此外，你的 DNS 服务器上必须具有引用此服务器的 MX 记录及 Internet SMTP 虚拟服务器的 IP 地址。



要提高双宿主服务器的安全性，应使用 Internet 协议安全（IPSec）策略筛选 Internet 网络接口卡上的端口，并严格限制允许登录到该服务器的用户。有关 IPSec 的详细信息，将在本系列的《网管员必读——网络安全》一书中详细介绍。

6.8.3 手动配置 Internet 邮件的发送

如果用户的邮件传递环境很庞大或者很复杂，那么用户自身将无法使用 Internet 邮件向导来配置 Exchange 以发送 Internet 邮件，而必须手动配置 Exchange 以处理通过 Internet 的出站邮件传递。配置 Exchange 以发送 Internet 邮件的过程包括下列任务。

- 确认 SMTP 虚拟服务器使用的是标准的 SMTP 端口（端口 25）。
- 配置一个用来路由 Internet 邮件的 SMTP 连接器。
- 确认 DNS 服务器可以解析外部名称，以便 SMTP 可以传递邮件。

本节说明如何在 Exchange 服务器上配置这些设置。

1. 验证 SMTP 虚拟服务器上的出站设置

前面已讨论，大多数 SMTP 所使用的出站设置是在 SMTP 连接器上配置的。但是，不能配置 SMTP 连接器以控制 Exchange 用来发送出站邮件的端口和 IP 地址。要控制这些端口和 IP 地址，必须配置 SMTP 虚拟服务器。在虚拟服务器上配置的 SMTP 连接器将继承这些设置。SMTP 虚拟服务器的两个属性直接与配置 Exchange 以发送 Internet 邮件相关。

1) 出站 TCP 端口

确保出站端口设置为端口 25（默认设置）。在与发送 Internet 邮件相关的两个设置中，这是必须验证的设置（注意，如果更改默认 SMTP 虚拟服务器上的默认设置，可能会导致邮件流出现问题）。

2) 使用外部 DNS 服务器

要发送 Internet 邮件，Exchange 使用的 DNS 服务器必须能够解析外部（Internet）名称。配置 DNS 解析外部名称的两种常见方法如下。

方法一：将 Exchange 配置为指向一个内部 DNS 服务器，而该内部 DNS 服务器使用指向外部 DNS 服务器的转发器（这是最简单也最常见的方法）。

方法二：将 Exchange 配置为指向一个内部 DNS 服务器，而该内部 DNS 服务器不包含指向外部 DNS 服务器的转发器，然后在 SMTP 虚拟服务器上配置一个负责发送外部邮件的外部 DNS 服务器。

下面具体介绍如何将确认出站 TCP 端口设置为 25，以及如何指定外部 DNS 服务器。

2. 确认用于传递邮件的出站端口设置为 25

（1）在 Exchange 系统管理器中展开“服务器”容器，再依次展开：服务器名→协议→SMTP，在“默认 SMTP 虚拟服务器”上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“传递”选项卡，如图 6-163 所示。

（2）单击【出站连接】按钮，打开如图 6-164 所示的对话框。确认 TCP 端口设置为 25。



图 6-163 “默认 SMTP 虚拟服务器属性”对话框“传递”选项卡

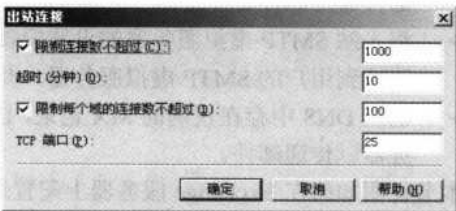


图 6-164 “出站连接”对话框



Internet 上的远程服务器希望用户的服务器使用 TCP 端口 25。建议不要更改此设置，因为其他 SMTP 服务器通常只接受端口 25 上的连接。

3. SMTP 虚拟服务器使用的外部 DNS 服务器

- (1) 在如图 6-163 所示的“默认 SMTP 虚拟服务器属性”对话框“传递”选项卡中，单击【高级】按钮，打开如图 6-165 所示的对话框。
- (2) 单击【配置】按钮，打开如图 6-166 所示的对话框。单击【添加】按钮以输入外部 DNS 服务器的 IP 地址。如果使用了多个外部 DNS 服务器，请使用【上移】或【下移】按钮设置 DNS 服务器的首选顺序。

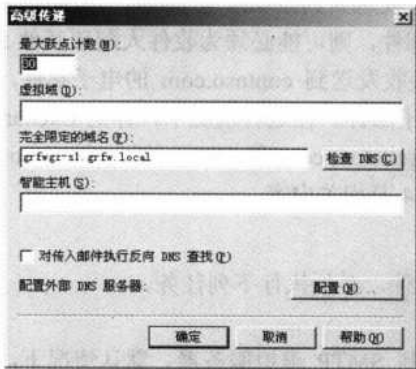


图 6-165 “高级传递”对话框

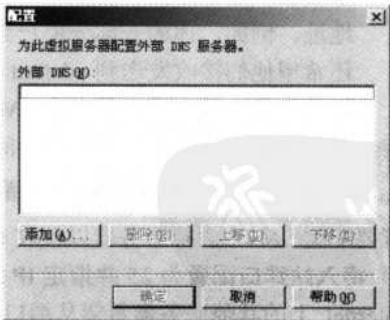


图 6-166 “配置”对话框

- (3) 配置好后依次单击【确定】按钮退出配置即可。这样 SMTP 默认虚拟服务器上就具有了能解析 Internet 域名的外部 DNS 服务器。

6.8.4 手动配置 Internet 邮件的接收

手动配置 Exchange 以接收 Internet 邮件的过程包括下列任务。

- 创建正确的收件人策略，以便 Exchange 服务器能够接收用户公司使用的所有电子邮件域的邮件。
- 将入站 SMTP 虚拟服务器的设置配置为允许匿名访问，以便其他 SMTP 服务器可以连接到用户的 SMTP 虚拟服务器，并向该虚拟服务器发送邮件。
- 确认 DNS 中存在正确的 MX 记录，以便 Internet 上的其他服务器可以找到用户的服务器以传递邮件。

本节说明如何在 Exchange 服务器上配置这些设置。

1. 配置收件人策略

Exchange 使用收件人策略来确定哪些邮件必须被接受，并在内部操作中被路由到组织中的邮箱。错误地配置收件人策略可能破坏邮件系统中的部分或全部收件人的邮件流。收件人策略在 Exchange 系统管理器中的“收件人”容器下的“收件人策略”中配置。

要确保正确配置收件人策略，应确认满足下列条件。

- 收件人策略不包含与组织中的任何 Exchange 服务器的完全限定域名（FQDN）相匹配的 SMTP 地址。例如，如果你有一个 FQDN 为 server01.contoso.com 的 Exchange 服务器，并且在任何收件人策略中都将此 FQDN (@server01.contoso.com) 作为 SMTP 地址和域名列出，那么此条目将阻止邮件路由到路由组中的其他服务器，因目的地址与源地址相同。
- 要接收的 SMTP 邮件所属的域已在收件人策略（默认策略或其他收件人策略）中列出。通过确认此信息，可以确保你的用户能够接收来自其他 SMTP 域的邮件。
- 配置了必要的 SMTP 电子邮件地址以接收发送到其他域的电子邮件。如果你当前并未接收发送到你的所有 SMTP 域的电子邮件，则可能必须为收件人配置其他 SMTP 地址。例如，你的一部分用户当前可以接收发送到 contoso.com 的电子邮件，但你还希望他们接收发送到 adatum.com 的电子邮件。在这种情况下，你的 Exchange 组织的收件人策略中必须存在 SMTP 地址 @adatum.com 和 SMTP 地址 @contoso.com。

有关收件人策略的详细信息，请参阅本章 6.7.4 节相关内容。

2. 配置入站 SMTP 虚拟服务器设置

若要配置 SMTP 虚拟服务器以接收 Internet 邮件，必须执行下列任务。

1) 将入站端口配置为 25 并指定 IP 地址

Internet 上的其他服务器希望从端口 25 连接到 SMTP 虚拟服务器。默认情况下，所有 SMTP 虚拟服务器都使用此端口。

2) 确认 SMTP 虚拟服务器允许匿名访问

要接收 Internet 邮件，SMTP 虚拟服务器必须允许匿名访问。Internet 上的其他服务器希望以匿名的方式与 SMTP 虚拟服务器通信，以便向用户发送 Internet 邮件。

3) 确认在 SMTP 虚拟服务器上配置了默认中继限制

在默认情况下，SMTP 虚拟服务器只允许已通过身份验证的用户中继电子邮件。此设置

会阻止未通过身份验证的用户使用 Exchange 服务器向外部域发送电子邮件。

下列过程说明了如何执行上述各项任务。

(1) 在 Exchange 系统管理器中，找到“默认 SMTP 虚拟服务器”选项。单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“常规”选项卡如图 6-167 所示。

(2) 单击【高级】按钮，打开如图 6-168 所示的对话框。在默认情况下，SMTP 虚拟服务器使用 IP 地址“所有未分配”，这意味着虚拟服务器在所有可用的 IP 地址上侦听请求。可以保留默认 IP 地址，或单击【编辑】按钮更改地址。在默认情况下，SMTP 虚拟服务器使用 TCP 端口 25。建议你不要修改默认端口分配。



图 6-167 “默认 SMTP 虚拟服务器属性”对话框“常规”选项卡

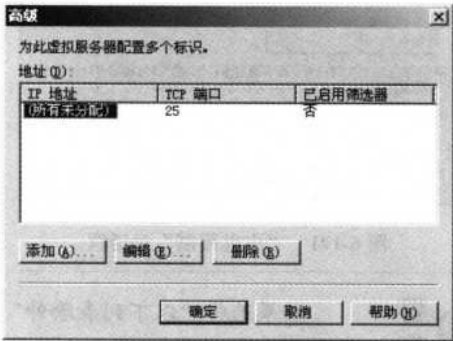


图 6-168 “高级”对话框

(3) 在如图 6-167 所示的对话框中，选择“访问”选项卡，如图 6-169 所示。单击【身份验证】按钮，打开如图 6-170 所示的对话框。



图 6-169 “默认 SMTP 虚拟服务器属性”对话框“访问”选项卡

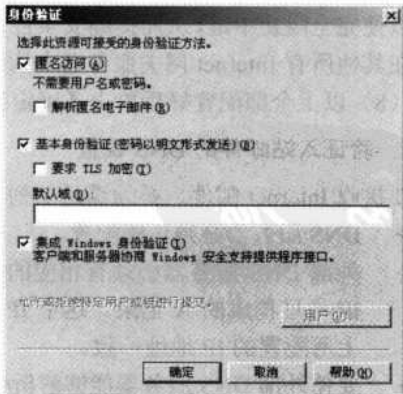


图 6-170 “身份验证”对话框

(4) 选中“匿名访问”复选项，单击【确定】按钮即可。

（5）如果确认 SMTP 虚拟服务器要开放中继，则同样在如图 6-169 所示的“访问”选项卡上，单击【中继】按钮，打开如图 6-171 所示的对话框。

（6）选择“仅以下列表”单选项，单击【添加】按钮，打开如图 6-172 所示的对话框。然后将允许其中继邮件的那些主机添加到列表中，以限制其他非法的邮件中继主机中继邮件。

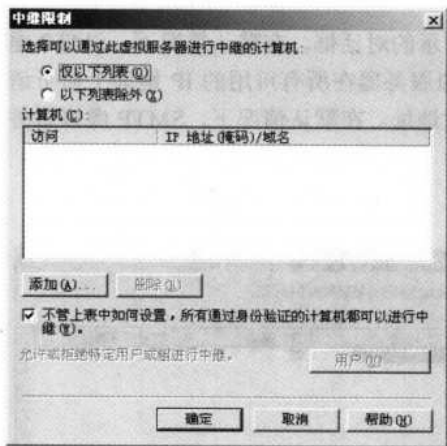


图 6-171 “中继限制”对话框

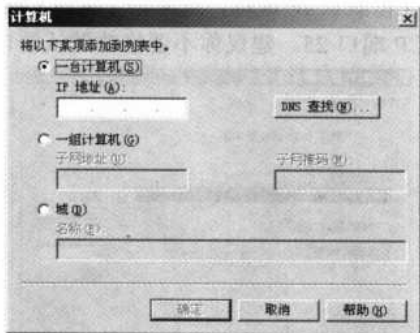


图 6-172 “计算机”对话框

警告 如果选择“以下列表除外”单选项，则未经授权的用户可能通过访问你的服务器在 Internet 上分发未经请求的电子邮件。

（7）选择“不管上表中如何设置，所有通过身份验证的计算机都可以进行中继”复选项。此设置允许你对未通过身份验证的所有用户拒绝中继权限。访问此服务器的任何远程 Internet 邮件访问协议版本 4（IMAP4）和邮局协议版本 3（POP3）用户都需通过身份验证才能发送邮件。如果你的用户都不需要通过 IMAP4 或 POP3 来访问此服务器，则可以清除此复选项以便完全阻止中继，从而提高安全性。还可以为 IMAP4 和 POP3 用户指定特定的服务器，然后在其他所有 Internet 网关服务器上清除此复选框。

（8）以上全部配置好后单击【确定】按钮即可完成。

3. 验证入站邮件的 DNS 设置

要接收 Internet 邮件，必须满足下列 DNS 设置要求。

- DNS 服务器必须正确配置。
- 外部 DNS 服务器必须有相应的 MX 记录，而该记录应当指向一条由邮件服务器的 IP 地址构成的 A 记录。这个 IP 地址必须与接收 Internet 邮件的 SMTP 虚拟服务器上所配置的 IP 地址一致。
- 要使外部 DNS 服务器能够解析你的邮件服务器的 MX 记录，并与邮件服务器联系，必须可以从 Internet 访问你的邮件服务器。
- 必须将 Exchange 服务器配置为使用可以解析外部 DNS 名称的 DNS 服务器。

要确保 MX 记录配置正确，可以使用 Nslookup 实用程序。要验证 Internet 上的其他服务

器是否可以通过端口 25 访问你的服务器，可以使用 Telnet。

6.9 地址列表

当用户使用客户端（如 Outlook）连接到 Exchange 时，他们希望可以很轻松地与组织中的其他人进行通信。此时，用户需要做的不仅仅是使用其邮件客户端撰写电子邮件。无论是发送电子邮件、给同事打电话、查找办公室号码，还是安排会议，他们都需要能够快速找到有关另一个收件人的信息。地址列表有助于用户以一种有意义的方式组织这种类型的信息。

6.9.1 地址列表概述

地址列表组织收件人，以便用户可以很轻松地找到想联系的收件人。最常用的地址列表是全局地址列表（GAL）。在默认情况下，GAL 中包含 Exchange 组织中的所有收件人。也就是说，安装了 Exchange Server 2003 的 Active Directory 目录林中的所有已启用邮箱或已启用邮件的对象都列在 GAL 中。要查找收件人的电子邮件地址或电话号码，用户可以使用 GAL 来找到此信息。为方便使用，GAL 是按名称而不是按电子邮件地址来组织的。

客户端应用程序（如 Outlook 2003）显示 Exchange 提供的可用地址列表，通常为“联系人”列表。当用户搜索信息时，将从可用地址列表中进行选择。有几个地址列表（如 GAL）是默认创建的。地址列表驻留在 Active Directory 中，因此与网络断开连接的移动用户也就与这些（服务器端）地址列表断开了连接。但是，可以创建脱机地址列表，以便在断开连接的环境中。这些脱机列表可以下载到用户的硬盘中。通常，为节省资源，脱机列表只包含驻留在服务器上的实际地址列表中的一部分信息。

Exchange 组织可以包含数千个收件人。编辑所有用户、联系人、已启用邮件的组和其他收件人可能会产生许多条目。作为管理员，可以创建地址列表来帮助组织中的用户更轻松地找到他们要找的信息。可以按照与收件人关联的任何属性对地址列表进行排序。可以用来筛选收件人的任何属性（城市、头衔、公司、办公楼等）都可以作为新地址列表的依据。还可以创建地址列表的子类别。例如，可以针对位于国内公司的所有同事创建一个地址列表（LocalList），而针对位于国外公司的所有同事创建另一个地址列表（ForeignList）。然后可以再在前面为国内公司同事创建的 LocalList 地址列表下针对具体在广东公司工作的所有人创建一个地址列表（GDList）。由于 GDList 是在 LocalList 列表下，因此 GDList 列表只能包含既在国内公司工作又在广东公司工作的那些收件人。

地址列表是动态创建的。当新的用户添加到组织中时，他们会自动被添加到所有相应的地址列表中。这些更新是收件人更新服务和 Exchange 系统助理的一项主要职责。

6.9.2 创建地址列表

地址列表对于用户来说可能是很有用的工具，但规划不当的地址列表可能会适得其反。创建地址列表前，首先要确保它对于用户有意义。应避免创建过多的地址列表，以至于用户不确定应在哪里查找收件人。应考虑对用户进行调查，以了解他们如何解释你所提议的地址

列表。最后，对地址列表命名并使该名称一目了然，以便用户只通过该名称就能立即知道可以找到哪些人员。当不确定时，应设置较少的地址列表，并提醒用户使用全局地址列表可以找到组织中的任何人。

在规划地址列表时，应考虑是否使用子类别。例如，可能要针对集团公司中各分支机构来设置地址列表，如图 6-173 所示中的“grfList”为集团公司地址总列表，下面的“grfwgzList”为广州子公司地址列表，而“grfwhljList”则为黑龙江子公司的地址列表。



图 6-173 含子类别的地址列表

为了进一步简化用户体验并组织列表，可以创建空地址列表。由于不会针对空地址列表创建查询，因此它不会返回收件人，正好可以充当组织其他列表的父容器。在前面的示例中，“grfwList”这个地址列表可以把它设为空地址列表，不具体添加收件人（具体的收件人在其中的两个子地址列表中）。

6.9.3 创建地址列表

地址列表的创建方法很简单，具体如下。

（1）在 Exchange 系统管理器中，展开“收件人”节点，找到“所有地址列表”子节点，或者其下的其他子节点，单击鼠标右键，在弹出的快捷菜单中选择【新建】下面的【地址列表】命令，打开如图 6-174 所示的对话框。在其中首先要为新建的地址列表起一个名。

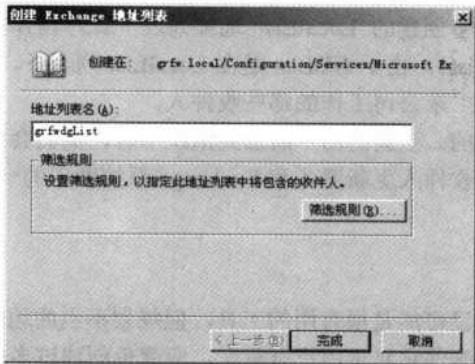


图 6-174 配置地址列表名称对话框

(2) 单击【筛选规则】按钮，打开如图 6-175 所示的对话框，适当地修改筛选器规则。在“常规”选项卡中可以指定收件人的类型（从中可以看出，还可以单独为启用了邮件功能的“公用文件夹”创建地址列表）；而在如图 6-176 所示“存储”选项卡中可以指定收件人所对应的邮箱。对于像这类要区别不同城市，甚至不同国家的地址列表，就必须在这里配置指定不同地址列表所包括的收件人邮箱服务器了（当然必须要求这些分公司的网络互联，否则无法指定。）通常是在同一公司的不同管理组，或者部门来划分地址列表的。

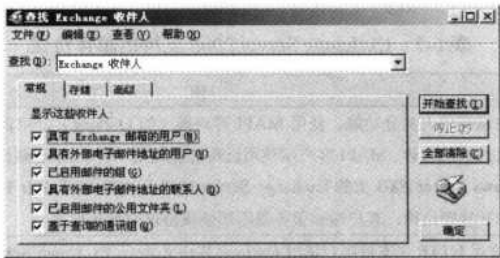


图 6-175 “查找 Exchange 收件人”窗口“常规”选项

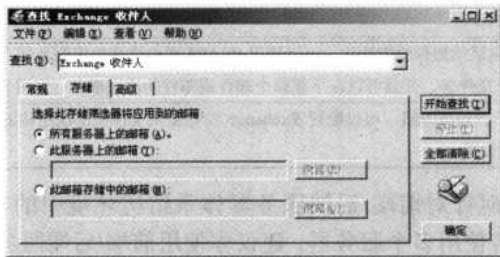


图 6-176 “查找 Exchange 收件人”窗口“存储”选项

除此之外，还可在如图 6-177 所示的对话框中更加详细地筛选相应地址列表的收件人。单击【字段】下拉按钮，在其中就列出了非常详细的可使用的筛选字段，然后在“条件”下拉列表框中选择所需满足的条件，还可在“值”列中配置筛选的相应字段的值，最后单击【开始查找】按钮，即可搜索全面满足如图 6-175、图 6-176 和图 6-177 所示 3 个对话框所设定的筛选条件的收件人。



图 6-177 “查找 Exchange 收件人”窗口“高级”选项

(3) 设定好后，单击【确定】按钮，返回到如图 6-174 所示的对话框。再单击【确定】按钮完成新的地址列表创建。

6.10 Exchange 客户端的设置

这里所讲的客户端设置其实就是 Exchange Server 2003 中所讲的用户代理设置。用户代理是收件人用来访问自己在 Exchange Server 服务器上的邮箱的邮件客户端。Exchange Server 2003 支持几个不同的客户端访问协议。表 6-3 列出了支持的邮件协议。

表 6-3 Exchange Server 2003 支持的邮件协议

协 议	描 述
MAPI	MAPI 客户端提供大部分功能。使用 MAPI 客户端（如 Outlook），可以访问邮箱以及默认公用文件夹存储中的所有文件夹的内容。MAPI 客户端使用远程过程调用（RPC）来连接到运行 Exchange Server 的服务器。运行在 Windows Server 2003 上的 Exchange Server 2003 还支持 RPC over HTTP。Windows Server 2003 提供 RPC over HTTP 基础结构。客户端和服务端不识别该协议的封装形式
HTTP	Exchange 使用 HTTP 来支持用户通过 Outlook Web Access、Exchange Active Sync 和 Outlook Mobile Access 访问邮件存储
POP3	POP3 是邮件检索协议，通过它可实现对 Exchange 的最基本访问。POP3 使用户可以访问其邮箱的收件箱文件夹中的邮件
IMAP4	IMAP4 是灵活的邮件检索协议。可以使用 IMAP4 客户端来组织服务器上的邮件，可以将邮件从一个文件夹移至另一个文件夹，并且可以在下载整个邮件或邮件的选定部分（如附件）之前预览邮件的内容
NNTP	NNTP 用于访问新闻组。可以配置 Exchange 发布公用文件夹层次结构的若干个部分，并使这些部分可供 NNTP 客户端使用

本节重点介绍了如何针对前端/后端服务器体系结构环境中的客户端访问对 Exchange Server 2003 进行管理。若使用多个服务器，建议你使用前端/后端服务器体系结构以满足所支持的客户端的不同邮件传递需求。

6.10.1 Outlook 2003 的客户端配置

Outlook 是目前绝大多数企业用户使用的邮件客户端软件，下面以最新的 Outlook 2003 为例向大家介绍客户端的具体配置方法。

（1）在运行 Outlook 2003 的计算机的“控制面板”的“经典视图”显示方式下，双击“邮件”选项（参见图 6-178），打开如图 6-179 所示的对话框。



图 6-178 “控制面板”中的“邮件”选项



图 6-179 “邮件设置——Outlook”对话框



注意

只有在安装了 Outlook 程序后才会显示“邮件”选项。Exchange 邮件账户的配置不能在 Outlook 2003 中创建，而需要从“控制面板”中双击“邮件”选项，在打开的对话框中创建。否则会出现“Outlook 正在运行，请退出”的错误提示，如图 6-180 所示。其他类型的邮件账户创建可以在 Outlook 中直接创建。



图 6-180 直接在 Outlook 中创建 Exchange 邮件账户时的错误提示

(2) 单击【电子邮件账户】按钮，打开如图 6-181 所示的对话框。选择“添加新的电子邮件账户”单选项。

(3) 单击【下一步】按钮，打开如图 6-182 所示的对话框。在这里要选择一个邮件服务器类型。此处因为是要创建 Exchange 邮件账户，所以选择“Microsoft Exchange Server”单选项。



图 6-181 “电子邮件”对话框



图 6-182 “服务器类型”对话框

(4) 单击【下一步】按钮，打开如图 6-183 所示的对话框。在这里要设置邮件账户所用的 Exchange Server 2003 服务器名，然后在用户名文本框中输入相应用户的邮件账户名，通常与用户在网络中的用户名一样，不用加上邮件域后缀。如 shelly@grfw.local 电子邮件地址，就可直接输入 shelly，而不用输入“@grfw.local”。



图 6-183 “Exchange Server 设置”对话框

如果用户当前系统不是采用相同账户登录，则会弹出如图 6-184 所示的对话框，要求输

412 网管员必读——网络应用（第2版）

入所创建邮件账户的用户信息才能向下进行。

(5) 单击【下一步】按钮，系统会弹出如图 6-185 所示提示框。在默认情况下，Exchange Server 服务器将该账户的所有邮件传递到该用户在 Outlook 2003 中的个人文件夹中，并提示更改设置的方法。



图 6-184 身份验证对话框

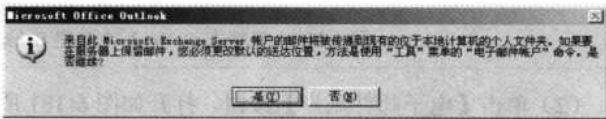


图 6-185 Outlook 系统提示框

如果要把邮件从服务器上下载到用户所用计算机 Outlook 个人文件夹中，则单击【是】按钮，否则单击【否】按钮，则邮件仍保留在邮件服务器上，在 Outlook 个人文件夹中没有用户的邮件。



如果在创建邮件账户时选择把邮件下载到用户个人文件夹中，但事后想要更改，要在服务器上保留邮件副本，则可在 Outlook 中执行【工具】→【电子邮件账户】菜单操作，首先打开的是如图 6-186 所示的对话框。选择“查看或更改现有电子邮件账户”单选项，单击【下一步】按钮，打开如图 6-187 所示的对话框。邮件存储位置就是在这个对话框的“将电子邮件投递到下列位置”下拉列表中选择。

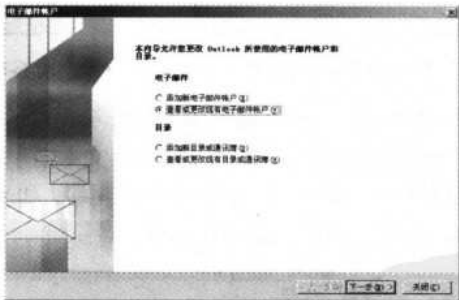


图 6-186 “电子邮件账户”对话框

“个人文件夹文件”是在你自己计算机上存储邮件和其他项目的数据文件。可以分配一个.pst 文件作为默认电子邮件的送达位置，也可以使用.pst 文件来备份项目以保护项目。“私人文件夹”是指在邮件服务器上的用户邮箱。如果要在服务器上保留邮件，则要在如图 6-187 所示的对话框中先选择相应的邮件账户，然后在“将电子邮件投递到下列位置”下拉列表框中选择“私人文件夹”选项。

(6) 在如图 6-185 所示的对话框中，单击【是 (Y)】按钮即把邮件传递到用户 Outlook 的个人文件夹中，通常采取这种设置，以使用户随时调阅，打开如图 6-188 所示向导对话框，

显示邮件账户创建成功。单击【完成】按钮即可。如果当前 Outlook 不能与 Exchange 邮件服务器连接成功，则会弹出如图 6-189 所示错误提示框。

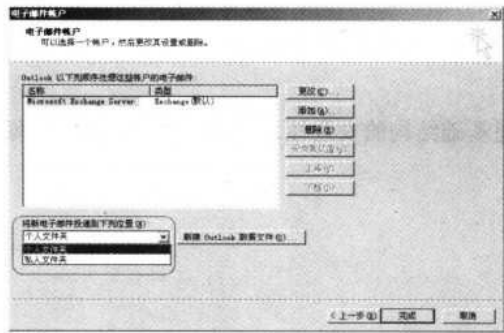


图 6-187 修改电子邮件账户对话框

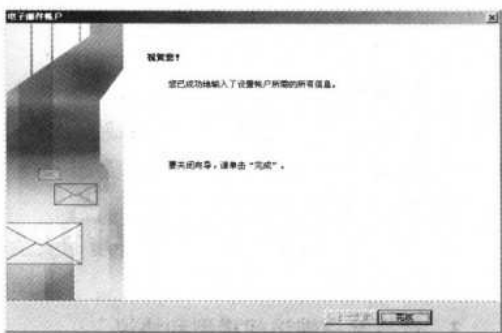


图 6-188 向导完成对话框



图 6-189 无法与 Exchange 邮件服务器连接成功时的错误提示

通过以上步骤，用户就创建了自己的 Exchange 账户，可以在 Outlook 2003 中收发内、外部邮件了（具体要根本 Exchange Server 2003 中的配置而定）。但要注意，在 Outlook 2003 中，一个用户只能创建一个 Exchange 邮件账户。如果用户有多个内、外部电子邮址，可以在用户属性对话框的“电子邮件地址”中添加，具体参见本章前面介绍。

6.10.2 准备管理客户端访问

在针对将支持的协议和客户端配置 Exchange 服务器上的设置之前，应确保已正确配置 Exchange 以满足特定的客户端访问需求。通常，要配置 Exchange 以实现客户端访问，必须完成下列步骤。

- 选择拓扑。
- 确保邮件传递基础结构的安全。
- 选择客户端访问模型和协议。
- 启用将支持的协议（可选）。
- 配置客户端和设备。

以下各主题简要讨论了上述每个步骤，并概述了每个步骤涉及到的内容及在制定与该步骤相关的决定时需考虑的因素。

1. 选择拓扑

如果你有多个 Exchange 服务器，并且计划允许从组织外部（Internet）访问 Exchange，那么必须了解推荐的 Exchange 前端/后端服务器体系结构。此服务器体系结构使用一个 Exchange 服务器处理所有来自客户端的请求，从而简化了具有多个 Exchange 服务器的组织

414 网管员必读——网络应用（第2版）

的客户端访问模式。前端服务器负责代理来自客户端的请求，并将这些请求传递给其上拥有邮箱的 Exchange 后端服务器。前端/后端服务器体系结构可能很简单，但也可能很复杂。不必再将 Exchange Server 2003 企业版用做前端服务器，可以在前端服务器上运行 Exchange Server 2003 标准版。

2. 配置客户端访问安全性

部署 Exchange 之前，应通过确保邮件传递基础结构的安全性，针对你将支持的客户端访问方法来准备组织，包括下列步骤。

- 更新服务器软件。
- 确保 Exchange 邮件传递环境的安全。
- 确保通信安全。

3. 选择客户端访问模型和协议

虽然简单邮件传输协议（SMTP）是 Exchange 的主邮件协议，但是与 Exchange 通信的客户端通常使用 SMTP 以外的协议。客户端可以使用邮局协议版本 3（POP3）、Internet 邮件访问协议版本 4（IMAP4）、HTTP 或网络新闻传输协议（NNTP）进行通信。一些客户端支持所有这些协议，而另一些则不然。为了适应协议使用方面的这些不同，Exchange 支持所有这些协议。这一全面的支持意味着在选择客户端访问模型时没有什么限制。确定哪一种客户端访问模型最适合用户的需要，然后就可以在 Exchange 中选择支持这一模型的协议。这些服务及 SMTP 是 Windows Server 2003 操作系统的一部分，并运行在 IIS 中的 Inetinfo.exe 进程下。

4. 配置客户端和设备

规划 Exchange 部署时需要确定哪些客户端对于组织中的用户是必要的。Exchange Server 2003 支持使用 MAPI、IMAP4、POP3、HTTP、SMTP 和 NNTP 的客户端。

客户端通常支持多个协议。例如，Outlook 2003 等客户端应用程序能够使用 MAPI、IMAP4、POP3 和 SMTP。但是，Microsoft Outlook Web Access、Outlook Mobile Access 和 Exchange Active Sync 客户端使用 HTTP。应根据用户选择支持的客户端，使用 Exchange 系统管理器或 IIS Microsoft 管理控制台（MMC）管理单元来管理客户端应用程序使用的协议。

如果用户使用 Exchange 中包括的任意客户端应用程序（Outlook Web Access、Outlook Mobile Access 和 Exchange Active Sync），则针对每种客户端存在不同的特定要求。

Outlook Web Access 要求在用户的计算机上具有支持的 Web 浏览器。

- Outlook Mobile Access 要求兼容的移动设备，例如 CHTML（CompactHTML）设备。
- Exchange Active Sync 要求基于 Microsoft Windows Mobile 的设备。

在选择客户端并针对客户端访问配置了 Exchange 后，Exchange 在如何管理对邮件传递基础结构的访问方面提供很大的灵活性。本节的后面部分描述了 Microsoft 支持进行客户端访问的客户端应用程序，并描述了如何管理这些应用程序。阅读这些部分可以了解如何管理与 Exchange 一起使用的客户端。

6.10.3 配置 Outlook 2003 缓存 Exchange 模式

Exchange Server 2003 和 Outlook 2003 构建在以前版本的 Exchange 和 Outlook 上，并在

客户端邮件传递方面进行了几项改进。

- Exchange 和 Outlook 现在只要求从客户端向服务器传递较少的信息，从而提高了性能，并改善了最终用户在慢速网络上的体验。
- Exchange 和 Outlook 现在支持使用 Windows RPC over HTTP 功能，从而使得 Outlook 2003 客户端可以使用 HTTPS 或 HTTP 直接连接到内部网络。

Exchange Server 2003 SP1 还新增以下功能：

- 将 Exchange 前端服务器指定为 RPC 代理服务器。
- 使客户端可以通过 RPC over HTTP 使用 Exchange 后端服务器。
- 将 Exchange 服务器指定为 RPC-HTTP 网络的一部分。
- Exchange 和 Outlook 现在包括缓存 Exchange 模式功能，从而可以借助 Outlook 实现真正的脱机访问。

缓存 Exchange 模式使用户可以使用其计算机上的本地邮箱副本，并借助 Outlook 2003 获得真正的脱机体验。也就是说，如果 Outlook 2003 客户端与 Exchange Server 2003 之间的网络连接断开，用户能够继续使用缓存的信息工作，而不会看到指出 Outlook 正在向 Exchange 服务器请求信息的弹出消息。

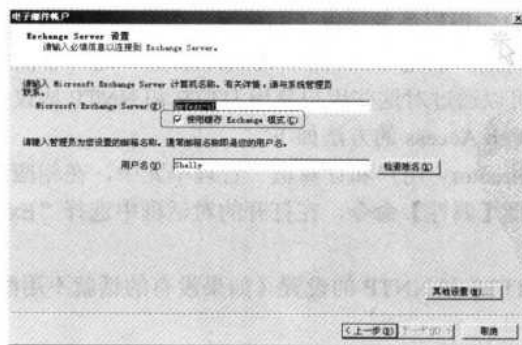
在默认情况下，新安装的 Outlook 2003 使用缓存 Exchange 模式。如果要从以前版本的 Outlook 升级到 Outlook 2003，并且希望用户能够使用缓存 Exchange 模式，必须手动配置 Outlook 客户端使用缓存 Exchange 模式。要进行此项操作，应修改用户的配置文件，让其使用 Exchange 邮箱的本地副本。

对 Outlook 2003 升级，手动启用缓存 Exchange 模式的方法如下。

（1）在运行 Outlook 2003 的计算机的“控制面板”的“经典视图”显示方式下，双击“邮件”选项（参见图 6-178），打开的对话框参见图 6-175。

（2）单击【电子邮件账户】按钮，打开如图 6-186 所示的对话框。选择“查看或更改现有电子邮件账户”单选项。

（3）单击【下一步】按钮，打开如图 6-187 所示的对话框。选择要修改的账户，然后单击【更改】按钮，打开如图 6-190 所示的对话框。



416 网管员必读——网络应用（第2版）

（4）在“Exchange 服务器设置”对话框中，选中“使用缓存 Exchange 模式”复选项，单击【下一步】按钮，返回到如图 6-186 所示的对话框。不过，此时原来的【下一步】按钮变成了【完成】按钮，单击它完成配置，保存对本地配置文件的更改。

6.10.4 使用 Outlook Web Access 访问

用于 Exchange Server 2003 的 Outlook Web Access 包括与用户界面和管理有关的重大改进。管理 Outlook Web Access 时，应使用 Exchange 系统管理器和 IIS 管理单元。下面具体说明这两个工具的使用。

- 使用 Exchange 系统管理器修改与 Outlook Web Access 访问控制有关的设置。
- 使用 IIS 管理单元控制用于 Outlook Web Access 虚拟目录（包括\Exchange、\Exchangeweb 和\Public）的【身份验证】设置。
- 使用 IIS 管理单元对 Outlook Web Access 启用 SSL。

以下说明了如何使用 Exchange 系统管理器和 IIS 管理单元执行与 Outlook Web Access 相关的各种管理任务。

1. 仅对内部客户端启用和禁用 Outlook Web Access

可以允许公司网络内的用户访问 Outlook Web Access，同时拒绝外部客户端的访问。此方法的关键是将收件人策略与专用的 HTTP 虚拟服务器结合起来使用。此方法的步骤如下。

（1）SMTP 域名创建一个收件人策略。连接到 HTTP 虚拟服务器的用户的电子邮件地址必须具有与虚拟服务器相同的 SMTP 域。创建收件人策略是对多个用户应用相同 SMTP 域的有效方法。具体参见本章前面 6.7.4 节介绍。

（2）将收件人策略应用于要允许访问的用户账户，具体参见 6.7.5 节。

（3）在前端服务器上创建一个新的 HTTP 虚拟服务器，以指定在收件人策略中使用的域。

完成上述步骤后，电子邮件地址与 HTTP 虚拟服务器具有不同 SMTP 域的用户将无法登录并访问 Outlook WebAccess。此外，只要你不将 SMTP 域用做默认域，外部用户将无法确定 SMTP 域，因为当用户向组织外发送电子邮件时，该域不会出现在“发件人”字段中。

除了对公司网络中的用户启用 Outlook Web Access 外，还可以阻止特定的内部用户访问 Outlook Web Access。可以通过对这些用户禁用 HTTP 和 NNTP 协议来完成此项操作。阻止内部用户访问 Outlook Web Access 的方法如下。

（1）在“Active Directory 用户和计算机”管理单元中，在相应用户上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“Exchange 功能”选项卡，如图 6-191 所示。

（2）禁用所有 HTTP 和 NNTP 的设置（如果没有的话就不用配置了），单击【确定】按钮退出即可。




图 6-191 用户属性对话框“Exchange 功能”选项卡

2. 使用浏览器语言

当使用 Microsoft Internet Explorer 5 或更高版本来访问 Outlook Web Access 时，新安装或升级的 Exchange Server 2003 将使用浏览器的语言设置来确定对信息（如电子邮件和会议请求）进行编码所用的字符集。

如果是从运行 Exchange 2000 Server，且已修改为使用浏览器的语言设置的服务器升级的，Exchange Server 2003 将继续以相同方式运行；如果预计组织中的 Outlook Web Access 用户会经常发送邮件，可以修改注册表设置，使运行 Internet Explorer 5 或更高版本的用户可以使用 UTF-8 编码的 UNICODE 字符来发送邮件。



警告

错误地编辑注册表可能导致严重的问题，甚至可能需要重新安装操作系统。因注册表编辑不当而导致的问题可能没有办法解决。在编辑注册表之前，请备份所有重要数据。

修改 Outlook Web Access 的默认语言设置的具体步骤如下。

- (1) 在 Exchange 服务器上，使用 Exchange 管理员账户登录，然后用本章前面介绍的方法启动注册表编辑器。
- (2) 在注册表编辑器中，找到下列注册表项：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEExchangeWEB\OWA\UseRegionalCharset
```

- (3) 单击鼠标右键，在弹出的快捷菜单中选择【DWORD 值】命令，创建一个名为“Use Regional Charset”的 DWORD 值。
- (4) 再在 UseRegionalCharsetDWORD 值项上单击鼠标右键，在弹出的快捷菜单中选择【修改】命令。在打开的“编辑 DWORD 值”对话框的“数值数据”文本框中键入 1，单击【确定】按钮退出设置。最后关闭注册表编辑器保存更改。

3. 设置登录页

可以在 Cookie 而不是浏览器中存储用户名和密码，对 Outlook Web Access 启用新的登录页。当用户关闭浏览器时，该 Cookie 将被清除。此外，如果一段时间未活动，该 Cookie 也

418 网管员必读——网络应用（第2版）

将被自动清除。新的登录页要求用户在访问电子邮件之前输入域、用户名和密码，或完整的用户主要名称（UPN）电子邮件地址和密码。

要启用此登录页，必须首先在服务器上启用基于表单的身份验证，然后通过设置 Cookie 超时期限，并调整客户端安全设置来确保登录页的安全。启用基于表单的身份验证的具体方法如下。

- （1）在 Exchange 服务器上，使用 Exchange 管理员账户登录，然后启动 Exchange 系统管理器。
- （2）在控制台树中展开“服务器”容器下要启用基于表单的身份验证的服务器节点下的“协议”选项，如图 6-192 所示。



图 6-192 Exchange 系统管理器“协议”选项

- （3）展开“HTTP”子节点，在“Exchange 虚拟服务器”选项上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“设置”选项卡，如图 6-193 所示。选择“启用基于表单的身份验证”复选项。



图 6-193 “设置”选项卡

- （4）单击【确定】按钮完成设置。

4. 设置 Cookie 身份验证超时

在 Exchange Server 2003 中，Outlook Web Access 用户凭据存储在 Cookie 中。当用户从 Outlook Web Access 注销时，Cookie 将被清除，并且对于身份验证而言不再有效。此外，在默认情况下，如果用户使用公用计算机，并在 Outlook Web Access 登录屏幕上选择了“公用

或共享计算机”选项，该计算机上的 Cookie 将自动在 15 分钟的用户未活动期后过期。

自动超时很有用，因为它有助于防止用户的账户受到未经授权的访问。但是，虽然自动超时极大地减小了未授权访问的风险，但并不能完全排除这样一种风险：如果 Outlook Web Access 账户在公用计算机上留下了一个仍在运行的会话，则未经授权的用户可以访问该账户。因此，必须教育用户采取预防措施来避免风险。

为了满足组织的安全需要，管理员可以在 Exchange 前端服务器上配置未活动超时值。要配置超时值，必须修改服务器上的注册表设置。

设置 Outlook Web Access 基于表单的身份验证中公用计算机的 Cookie 超时值的具体步骤如下。

(1) 在 Exchange 前端服务器上，使用 Exchange 管理员账户登录，然后用本章前面介绍的方法启动注册表编辑器。

(2) 在注册表编辑器中，找到下列注册表项：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA

(3) 在表项上单击鼠标右键，在弹出的快捷菜单中选择【新建】下的【DWORD 值】命令，在详细信息窗口中，将新的值命名为 PublicClientTimeout。

(4) 在新建的“Public Client Timeout DWORD”值项上单击鼠标右键，在弹出的快捷菜单中选择【修改】命令，在打开的对话框的“基数”栏中选择“十进制”单选项；在“数值数据”文本框中键入 1~432000 之间的一个值（分钟）。

(5) 最后单击【确定】按钮完成设置。



设置 Outlook Web Access 基于表单的身份验证中信任计算机的 Cookie 超时值的具体步骤与上面介绍的公用计算机超时值配置方法基本一样，只是创建的“DWORD”值项不一样，此处要命名为 Trusted Client Timeout。值也是 1~432000（分钟）之间的一个值。

6.10.5 在 Outlook 中创建公用文件夹

在 Exchange 系统管理器中配置了公用文件夹，其目的就是为所属用户提供类似文件共享的功能。当然，公用文件夹不仅可以提供文件共享，还可以通过启用邮件功能起到邮件组的作用，用来统一收、发所属用户公共的电子邮件。共有用户通过 Outlook 可以直接查看所属公用文件夹中的文件和邮件。

1. 创建公用文件夹

在 Outlook 中创建与配置公用文件夹的方法很简单，只需在 Outlook 中执行【文件】→【新建】→【文件夹】菜单命令，打开如图 6-194 所示的对话框。在“名称”文本框中配置新建公用文件夹名称，这里的名称一定要与相应用户在 Exchange 邮件服务器上有权创建的公用文件夹一致。然后单击【确定】按钮，即可完成公用文件夹的创建。

此功能要求使用 Microsoft Exchange 账户，并且管理员要为相应用户配置允许创建公用文件夹的权限。

若要创建公用文件夹，必须具有在现有公用文件夹中创建文件夹的权限。如果用户没有

420 网管员必读——网络应用（第2版）

在 Exchange 邮件服务器上配置允许创建公用文件夹的权限，则在单击【确定】按钮后会弹出如图 6-195 所示错误提示框。

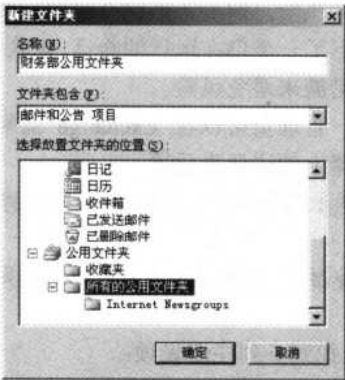


图 6-194 “新建文件夹”对话框

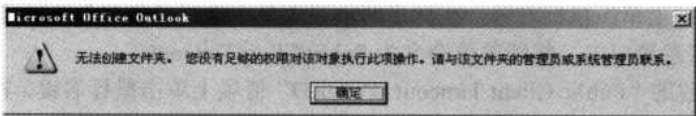


图 6-195 用户没权限创建公用文件时的错误提示

管理员为用户配置创建公用文件夹权限的方法是在 Exchange 系统管理器中，找到相应的公用文件夹，单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，然后在打开的对话框中选择“安全”选项卡，如图 6-196 所示。在其中把相应用户添加进去。当然如果相应用户已是系统默认允许的几个组中的成员就不用再添加了。关键是要在下面的权限列表中允许“Create public folder”（创建公用文件夹）权限项。



图 6-196 “安全”选项卡

2. 查看和使用公用文件夹

创建了的公用文件，默认是没有显示的。要在 Outlook 窗口中执行【转到】→【文件夹

列表】菜单命令，此时就会在 Outlook 窗口中看到所创建的公用文件夹了，如图 6-197 所示。



图 6-197 在 Outlook 中显示的公用文件夹

6.11 邮件服务器管理

6.11.1 管理收件人权限

Exchange Server 2003 组织中的收件人通过 Active Directory 中的收件人对象来表示。Exchange Server 2003 组织包含下列 5 种类型的收件人对象。

1) 已启用邮箱的用户账户

已启用邮箱的用户是 Exchange Server 2003 组织中最常见的收件人对象。已启用邮箱的用户是在运行 Exchange Server 的服务器上拥有邮箱的 Windows 用户。已启用邮箱的用户账户是被分配了唯一安全标识符(SID)的 Active Directory 对象。此标识符使用户可以访问 Active Directory 域中的资源。一旦用户账户成为了已启用邮箱的账户，就会在运行 Exchange Server 的服务器上拥有邮箱。这样，用户便可以使用所支持的客户端（如 Office Outlook）发送和接收电子邮件。

2) 已启用邮件的用户账户

已启用邮件的用户具有电子邮件地址，但在运行 Exchange Server 的服务器上没有邮箱。已启用邮件的用户账户具有 SID，并且可以访问 Active Directory 域中的资源，但是用来对用户账户启用邮件功能的电子邮件地址引用的是外部邮件系统或非 Exchange 邮件系统中的邮箱。已启用邮件的用户账户在全局地址列表中列出。

3) 已启用邮件的联系人

已启用邮件的联系人没有 SID，因此在 Exchange 组织中没有 Exchange 邮箱，这意味着已启用邮件的联系人无法访问域中的资源，但是收件人对象会出现在全局地址列表中。发送给联系人的电子邮件会被路由到与该联系人对象关联的电子邮件地址。

4) 已启用邮件的组

已启用邮件的组是配置了电子邮件地址的用户、组和联系人的集合。通用组和安全组均可以成为已启用邮件的组，但建议仅仅将通用组用于电子邮件功能。已启用邮件的组通常被

422 网管员必读——网络应用（第2版）

称为通信组列表，因为被分配了电子邮件地址。在邮件发送到该组后，Exchange Server 2003 展开组成员，并将邮件分别传递给每一个收件人。Exchange Server 2003 支持基于查询的通信组的使用。所谓基于查询的通信组，是指其成员由轻型目录访问协议（LDAP）查询确定的通信组列表。

5) 已启用邮件的公用文件夹

已启用邮件的公用文件夹是用户可以向其中发送电子邮件的公用文件夹。已启用邮件的公用文件夹具有唯一的电子邮件地址，并且可以显示在全局地址列表中。

管理收件人包括创建收件人、使用收件人策略为收件人分配电子邮件地址，以及使用“Active Directory 用户和计算机”管理收件人对象的设置等。

管理 Exchange 组织时，一些最为重要的安全任务将涉及到权限。在 Exchange Server 2003 中，正确地管理权限确保了用户和管理员能够成功地完成他们必须执行的那些任务，同时防止用户和管理员有意或无意地执行不适当的任务。

在 Exchange Server 2003 中，可以管理的权限有 3 组。

- Exchange 对象的权限：这些设置存储在 Active Directory 和 Internet 信息服务（IIS）元数据库中。
- 存储权限。
- NTFS 文件系统卷上的文件权限。

这些权限共同提供了在 Exchange Server 2003 安装中的所有元素上实现安全性的方法。

本节集中讲述了使用 Exchange 系统管理器管理 Active Directory 和 IIS 元数据库中的 Exchange 对象的权限。有关管理存储权限的详细信息，将在 6.11.3 节“管理邮箱存储和公用”中介绍。有关了解和管理 NTFS 权限的详细信息，请参阅本系列图书《网管员必读——网络管理》一书。

1. Exchange 权限管理方式

安装的 Exchange 软件中的大多数元素都是通过对象来表示的。例如，服务器本身、SMTP 虚拟服务器，以及邮箱存储都表示为对象。对其中每个对象的控制都是通过一组安全权限来实现的。Exchange Server 2003 中对象的权限是基于 Windows 操作系统通过 Active Directory 和 IIS 实现的权限构建的。Exchange Server 2003 使用 Active Directory 和 IIS 元数据库来存储有关 Exchange 对象的权限信息。

考虑到有关 Exchange 对象的信息存放在两个位置这一事实，应使用 Exchange 系统管理器来管理这些对象。这一工具统一表示存储在 Active Directory 和 IIS 元数据库中的对象。因此，可以通过一个界面管理存储在两个位置的对象。

Exchange 系统管理器暴露的权限模型是基于 Windows 安全模型构建的，后者是基于随机访问控制概念的面向对象安全模型。这意味着每个 Exchange 对象都有它自己的独立权限（以便控制对该对象的访问），并且这些权限可以由具有适当权限级别的任何人管理。此权限模型使得在安全策略要求进行委派的环境中实现委派的权限模型成为可能，即根据特定角色执行的功能性任务，为其分配不同的权限。

但是，使得 Exchange 满足复杂安全要求的大量对象和权限，也使管理工作看上去很复杂。幸运的是，Exchange 系统管理器通过下列功能简化了权限管理。

- 支持继承。

- 标准安全角色。
- Exchange 管理委派向导。

这些功能一起发挥作用，简化了权限的管理，以至于大多数 Exchange 对象都可以实现它们的安全要求，而不必对各个对象的各个属性设置权限。

2. “继承”的价值

在 Windows 中，“继承”描述的是这样一个过程：对象在创建时默认情况下继承其父对象的权限，这在配置 Windows 系统中的用户权限和 NTFS 文件权限时经常遇到。继承简化了在 Exchange 系统中管理权限的任务，这表现在下列方面。

- 它使得无须在创建子对象时手动对其应用权限。
- 它确保了附属于父对象的权限以一致的方式应用于所有子对象。
- 如果必须修改某个容器内所有对象的权限，只需更改一次该容器的权限。容器内的对象将自动继承更改。

对于某些 Exchange 对象，可以自定义此继承。这些对象包括公用文件夹树、地址列表和邮箱存储。对于这些对象，可以指定子对象不继承权限。或者，可以指定下列容器或子容器继承权限。

- 仅此容器。
- 此容器及所有子容器。
- 仅子容器。

继承使得在对象的层次结构中以一致的方式应用权限成为可能。就继承本身而言，它是一个简化权限应用的重要工具。

3. Exchange 中标准安全角色的价值

为了帮助简化权限管理过程，Exchange Server 2003 提供了 3 个预定义的安全角色，可以在 Exchange 管理委派向导中使用这些角色。这些角色是标准权限的集合，可以应用在组织或管理组级别。账户或组应用这些角色后，将立即被授予相应对象上的一组标准权限。角色十分依赖于权限继承，以确保权限的应用保持一致。应用角色后，与该角色关联的标准权限通过继承应用到层次结构中的下级对象。

由于设计角色是为了满足 Exchange 部署中常见的安全要求，因此应尽可能多地尝试使用这些角色。

Exchange Server 2003 提供的标准安全角色有以下几种。

1) Exchange 管理员（完全控制）

该角色对 Exchange 系统信息具有完全管理权限，并可以修改权限。此角色适用于必须能够修改权限及查看和管理 Exchange 配置信息的人员。


2) Exchange 管理员

该角色对 Exchange 系统信息具有完全管理权限。该角色不同于 Exchange 管理员（完全控制）。主要区别是该角色不能修改权限。该角色适用于必须能够查看和管理 Exchange 配置信息，而不需要能够修改权限的人员。

3) Exchange 管理员（仅查看）

该角色可以查看，但不能管理 Exchange 配置信息。该角色适用于必须能够查看 Exchange 配置信息，而不需要能够更改该配置信息的人员。与 Exchange 管理员角色一样，该角色也不

能修改权限。


**注意**

不要将 Exchange 安全角色与 Active Directory 中的安全组弄混。角色是应用于 Active Directory 中的用户或组的一组标准权限。可以将角色想象成模板，而不要想象成安全组。

由于这些角色是一组标准权限，与安全组不同，角色具有相互取代的固有特性，因此，没有必要同时应用较高级和较低级的特权角色，应用较高级特权角色已足够。应用于组织的角色和应用于管理组的角色稍有不同。因此，应用角色后所导致的有效权限也可能稍有不同。表 6-4 列出了有效权限（基于应用的角色以及应用的位置），适用于“在管理组级别应用的角色在管理组级别应用后的有效角色”、“在组织级别应用的角色在管理组级别应用后的有效角色”和“在组织级别应用的角色在组织级别应用后的有效角色”3 种情形。这些表说明了角色是如何相互取代的，以及在组织级别和管理组级别产生的不同影响。

表 6-4 基于应用的角色及其相应级别应用后的有效角色

被授予的 Exchange 管理员角色	有效的 Exchange 管理员角色		
	仅查看	管理员	管理员（完全控制）
Exchange 管理员（仅查看）	是	否	否
Exchange 管理员	是	是	否
Exchange 管理员（完全控制）	是	是	是

**说明**

没有表示在管理组级别应用的角色在组织级别应用后的有效角色。这是因为在管理组级别应用的角色只适用于本地管理组。由于管理组位于层次结构中组织级别的下面，因此管理组可以继承组织的权限，但反过来则不成立。

4. Exchange 管理委派向导的价值

Exchange 管理委派向导在 Exchange 系统管理器中的组织级别，或管理组级别应用标准安全角色。需要记住的一点是，Exchange 管理委派向导以一致的方式对 Exchange 层次结构中的对象应用经过认真测试的权限。由于权限应用的这种一致性，因此该向导是在 Exchange 环境中管理权限的推荐和首选的方法。可以对各个对象应用自定义权限，但前提是安全策略允许这样做，并且是在完成测试之后。手动创建自定义权限增加了出现人为错误的可能性。还增加了由于误解权限的工作原理而创建不适当权限的可能性。此外，自定义的安全设置需要更多的维护，因为必须对它们进行存档，并且必须对自定义设置进行检验。虽然在某些情况下自定义安全设置是适宜的，但是必须认真地权衡风险和成本。

可以从组织级别，或管理组级别启动 Exchange 管理委派向导。本节前面的“Exchange 中标准安全角色的价值”已指出，与角色关联的权限将在层次结构中从启动该向导时所在的对象向下应用。例如，如果在组织级别启动该向导，与角色关联的权限将应用于层次结构中组织以下的所有对象，包括所有的管理组。或者，如果在管理组启动该向导，与角色关联的权限将只应用于该管理组中的对象。

当启动 Exchange 管理委派向导时，它会提示你指定要将安全角色应用于哪些用户和组。通常，建议你将用户放入安全组内，然后使用向导对这些组应用角色。对各个用户应用权限很快就会使得管理工作变得很困难。

向导完成后，Exchange 系统管理器将权限应用于层次结构（向导启动时所处的位置）中选定的组或用户。权限将通过继承在层次结构中向下传播。通过使用该向导，只需若干次单击操作便可对 Active Directory 和 IIS 元数据库中的 Exchange 对象设置所有权限。

6.11.2 Exchange 管理委派向导

Exchange 管理委派向导简化了为 Exchange 管理员委派权限的过程。可以在系统管理器的组织级别委派管理权限，也可以在管理组级别委派权限。所设置的权限的作用域由向导的启动位置决定。如果从组织级别启动向导，则指定的组或用户将具有组织级别的管理权限。如果从管理组级别启动向导，则指定的组或用户将具有管理组级别的管理权限。

若要使用 Exchange 管理委派向导，请执行下列操作（以在组织级别上执行为例）。

（1）执行【开始】→【所有程序】→【Microsoft Exchange】→【系统管理器】菜单操作，启动 Exchange Server 2003 的系统管理器。

（2）在控制台树中，选择要为其委派管理权限的组织或管理组，单击鼠标右键，在弹出的快捷菜单中选择【委派控制】命令，打开如图 6-198 所示的对话框。

（3）单击【下一步】按钮，打开如图 6-199 所示的对话框。在“用户或组”对话框中，单击【添加】按钮，打开如图 6-200 所示的对话框。

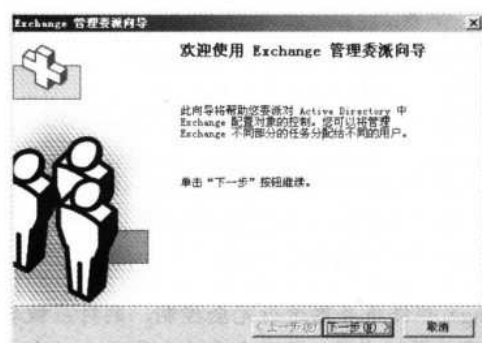


图 6-198 “欢迎使用 Exchange 管理委派向导”对话框

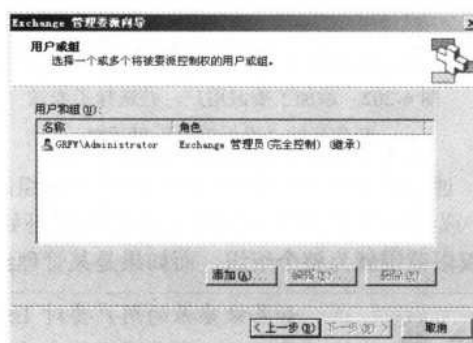


图 6-199 “用户或组”对话框

（4）单击【浏览】按钮，打开如图 6-201 所示的对话框。在其中输入，或者查找经委派管理权限的相应用户或组账户。确定后单击【确定】按钮，将管理权限授予新的用户或组。回到如图 6-198 所示的对话框中后，再在“角色”下拉列表框中选择要委派的一种管理员角色类型，具体角色所具有的权限参见 6.10 介绍。选择好后单击【确定】按钮，此时的图 6-199 就变为如图 6-202 所示了。



注意

如果被委派的是对相应邮件服务器具有完全控制权限，则该用户，或组账户必须是本地邮件服务器的管理员组成员，否则委派将不成功。但如果是仅具有查看权限类型的管理员角色，则可以是任何普通的用户，或组账户。

（5）单击【下一步】按钮，打开向导完成对话框，如图 6-203 所示。在其中显示了上几步所委派的用户，或组账户，以及相应角色类型。

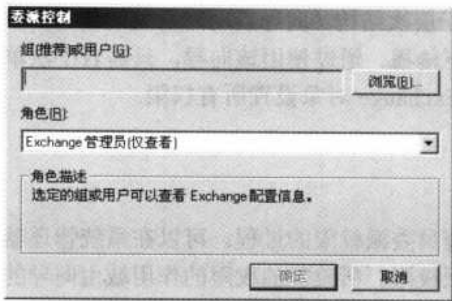


图 6-200 “委派控制”对话框

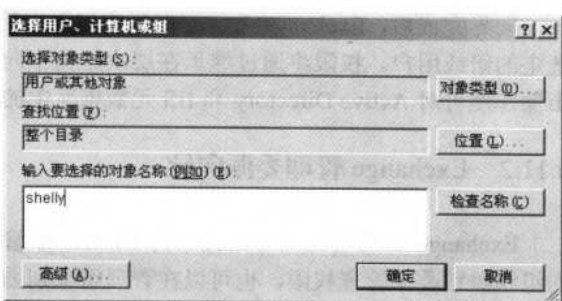


图 6-201 “选择用户、计算机或组”对话框

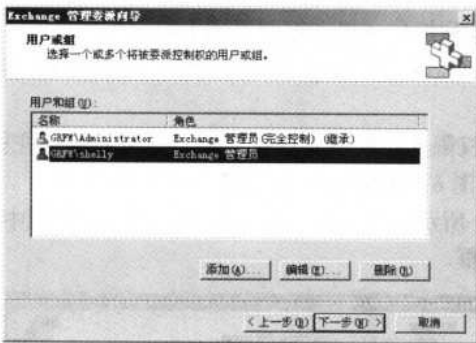


图 6-202 添加了委派用户，并选择了委派角色后的“委派控制”对话框

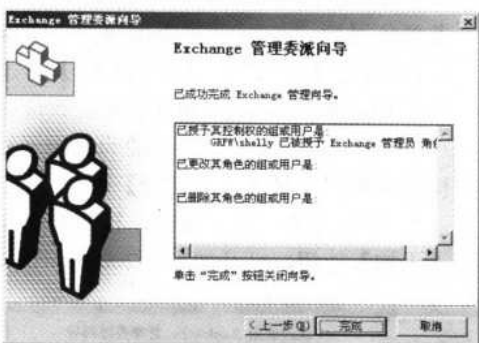


图 6-203 向导完成对话框

通过以上 5 步就完成了用户，或组账户的管理委派过程。要注意的是，被委派的用户，或组账户所具有的权限范围是由委派开始时所选择的单位级别来定的，如果是组织级别，则权限范围就为整个组织，而如果是某管理组，则权限只局限于某个对应的管理组。



如果被委派的用户要对 Exchange 邮件服务器进行完全控制，则对应被委派的用户还必须是域网络中的系统管理员组成员。否则在委派向导结束时会出现如图 6-204 所示警告提示框。

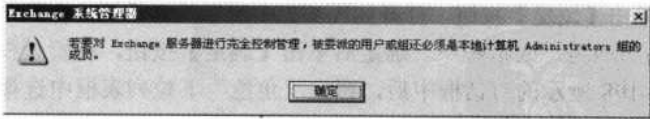


图 6-204 “Exchange 系统管理器”警告提示框

6.11.3 管理邮箱存储和公用文件夹存储

用户邮箱和公用文件夹是 Exchange Server 2003 的两个重要邮件存储位置，邮箱用来存储用户的私人邮件，而公用文件夹则用来存储所有用户公用的文件，其中可以是邮件，也可以是消息。

1. 管理邮箱存储和公用文件夹存储的方法

可以使用下列方法管理邮箱存储。

- 查看登录和邮箱信息。
- 更改创建存储时设置的任何属性。
- 对邮箱存储应用策略。
- 在邮箱存储中运行全文索引。

可以用下列任一方法管理公用文件夹存储。

- 查看登录信息、公用文件夹信息、公用文件夹实例信息，以及复制状态信息。
- 更改创建存储时设置的任何属性。
- 应用策略。
- 对公用文件夹存储使用全文索引。

2. 查看邮箱存储和公用文件夹存储

若要查看登录和邮箱信息，请执行下列操作。

- (1) 在 Exchange 系统管理器中导航到要管理的邮箱存储，如图 6-205 所示。



图 6-205 “邮箱存储”在系统管理器中的位置

- (2) 打开邮箱存储容器，然后选择“登录”选项。有关每次登录存储的信息都将显示在详细信息窗口中。在“登录”选项上单击鼠标右键，在弹出的快捷菜单中选择【查看】下的【选择列】命令，查看可用于构造视图的信息。表 6-5 描述了可用的列。

表 6-5 “邮箱存储”项中的“登录”选项可用的列

列 标 题	描 述
用户名	网络用户名
Windows 2000 账户	最后一次登录到该邮箱的用户的 Windows 账户名
登录时间	用户最后一次登录的日期和时间
上次访问时间	用户最后一次访问邮箱存储的日期和时间
客户端版本	登录该邮箱或公用文件夹所用的客户端版本
代码页	客户端使用的代码页
文件夹操作数	最后 60 秒执行的文件夹操作（如打开或关闭文件夹）总数
完整邮箱目录名	已在访问的邮箱的完整电子邮件地址。此选项只用于邮箱存储
完整用户目录名	已在访问邮箱存储的邮箱的名称
主机地址	客户端的 IP 地址

(续表)

列标题	描述
区域设置 ID	客户端使用的语言的区域设置 ID
邮件操作数	最后 60 秒执行的邮件操作（如打开或关闭邮件）总数
打开的附件数	打开的附件总数
打开的文件夹数	打开的文件夹总数
打开的邮件数	打开的邮件总数
其他操作数	最后 60 秒执行的其他操作的总数
进度操作数	最后 60 秒执行的进度操作的总数。进度操作提示用户完成一项任务需要的时间
流操作数	最后 60 秒执行的流操作（如查看或更改附件）总数
表操作数	最后 60 秒执行的表操作（如查看文件夹内容）总数
操作总数	最后 60 秒执行的操作总数
传输操作数	最后 60 秒执行的传输操作（如复制或移动邮件）总数

（3）再在邮箱存储容器中的“邮箱”上单击鼠标右键，在弹出的快捷菜单中选择【查看】下的【列表】命令，查看可用于构造视图的信息。表 6-6 描述了可用的列。

表 6-6 “邮箱存储”项中的“邮箱”选项上可用的列

列标题	描述
邮箱	该邮箱的名称。包括在默认的列视图中
上次登录用户	最后一次登录到此邮箱的用户的 Windows 账户名
大小（KB）	该邮箱在邮箱存储中占用的磁盘空间总量（KB），包括邮件、附件，以及关联邮件表单中的隐藏系统信息所占用的空间
项目总计	存储在邮箱中的非关联邮件的总数
上次登录时间	用户最后一次登录到该邮箱的时间
上次注销时间	用户最后一次从该邮箱注销的时间
已删除邮件（KB）	该邮箱中已删除但保留的邮件占用的磁盘空间总量（KB）
存储限制	该邮箱相对于存储限制的状态
相关邮件总计	邮箱中表示隐藏系统信息（如表单、规则、视图、答复模板，以及延迟操作邮件）的邮件的总数
完整邮箱目录名	邮箱 GUID 所在 Active Directory 配置容器位置的可分辨名称
断开时间	Exchange 检测到用户从邮箱删除或断开连接（邮箱不再与用户关联）的日期和时间

若要查看公用文件夹存储的登录信息，请执行下列操作。

（1）启动系统管理器，在如图 6-205 所示控制台窗口中导航到要管理的“公用文件夹存储”节点上，如图 6-206 所示。



图 6-206 “公用文件夹存储”在系统管理中的位置

(2) 单击“登录”选项。有关每次登录公用文件夹存储的信息都将显示在详细信息窗口中。在“登录”选项上单击鼠标右键，在弹出的快捷菜单中选择【查看】下的【选择列】命令，查看可用于构造视图的登录信息类型。具体可用的列如表 6-7 所示。

表 6-7 “公用文件夹存储”项中的“登录”选项可用的列

列标题	描述
用户名	网络用户名
Windows 2000 账户	最后一次登录到该邮箱的用户的 Windows 账户名
登录时间	用户最后一次登录的日期和时间
上次访问时间	用户最后一次访问存储的日期和时间
客户端版本	登录该邮箱或公用文件夹所用的客户端版本
代码页	客户端使用的代码页
文件夹操作数	最后 60 秒执行的文件夹操作（如打开或关闭文件夹）总数
完整邮箱目录名	已在访问的邮箱的完整电子邮件地址。此选项只用于邮箱存储
完整用户目录名	正在访问邮箱存储的邮箱的名称
主机地址	客户端的 Internet 协议（IP）地址
区域设置 ID	客户端所使用的语言的区域设置 ID
邮件操作数	最后 60 秒执行的邮件操作（如打开或关闭邮件）总数
打开的附件数	打开的附件总数
打开的文件夹数	打开的文件夹总数
打开的邮件数	打开的邮件总数
其他操作数	最后 60 秒执行的其他操作的总数
进度操作数	最后 60 秒执行的进度操作总数。进度操作提示用户完成一项任务需要的时间
流操作数	最后 60 秒执行的流操作（如查看或更改附件）总数
表操作数	最后 60 秒执行的表操作（如查看文件夹内容）总数
操作总数	最后 60 秒执行的操作总数
传输操作数	最后 60 秒执行的传输操作（如复制或移动邮件）总数

有关“邮箱存储”和“公用文件夹存储”属性的配置在本章前面已有介绍，参照即可。至于策略的应用将在本章后面具体集中介绍。“全文索引”方面的内容在大多数企业邮件系统中很少用到，故不作介绍。

6.11.4 使用队列查看器管理邮件

队列查看器是 Exchange 系统管理器中的一项功能，借助此项功能可以监视组织的邮件队列及这些队列中所包含的邮件。队列查看器工作在服务器级别。在 Exchange 系统管理器中，展开服务器，然后单击“队列”子节点，打开队列查看器，并显示与该服务器关联的邮件队列，如图 6-207 所示。



图 6-207 Exchange Server 2003 中的队列查看器

1. 邮件查看器概述

在 Exchange Server 2003 中，队列查看器的功能得到了增强，以改善对邮件队列的监视。在 Exchange Server 2003 中，可以从每个服务器下的“队列”节点中查看特定服务器的所有邮件队列。这是在 Exchange 2000 基础上进行的改进。在 Exchange 2000 中，每个协议虚拟服务器都有它自己的“队列”节点，用户无法从一个中心位置查看服务器上的所有队列。例如，使用 Exchange Server 2003 可以使用队列查看器查看服务器上的 X.400 和 SMTP 队列，而不必分别在其各自的协议节点中查看这些队列。

Exchange Server 2003 中队列查看器的其他增强功能包括以下几方面。

- 禁用出站邮件：可以使用一个名为“禁用出站邮件”的选项来禁用所有 SMTP 队列中的出站邮件。方法是单击其中的【禁用出站邮件】按钮。
- 设置刷新速率：可以使用“设置”选项设置队列查看器的刷新速率。方法是在如图 6-207 界面中单击【设置】按钮，打开如图 6-208 所示的对话框。在这里可以设置刷新速率。
- 查找邮件：可以使用如图 6-207 所示界面中的【查找邮件】按钮来基于发件人、收件人和邮件状态搜索邮件。此选项与 Exchange 2000 队列查看器中的邮件枚举功能类似。方法是单击【查看邮件】按钮，打开如图 6-209 所示的对话框。在这里可以查看特定邮件。



图 6-208 “设置”对话框

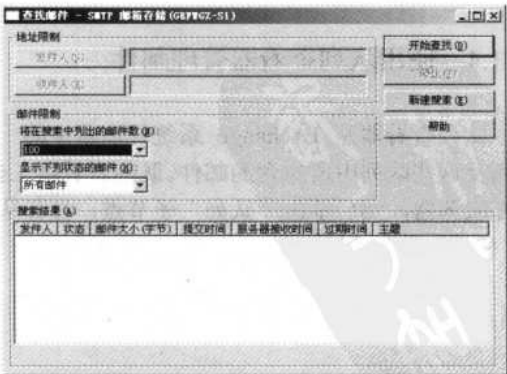


图 6-209 查找邮件—本地传递窗口



注意

在查看邮件时，一定要先在队列中定位相应的邮件查看器队列，然后再单击【查找邮件】按钮，打开如图 6-209 所示的对话框。并在这个对话框中输入对应队列中的发件、收件人等查看条件，否则查到的可能不是想要查找的邮件。也可直接双击相应队列，打开如图 6-209 所示的对话框进行邮件查找。

- 查看其他信息：可以单击特定队列以查看有关该队列的其他信息。
- 查看以前被隐藏的队列：Exchange Server 2003 中的队列查看器显露了在 Exchange 2000 中不可见的 3 个队列：“暂缓提交的 DSN 邮件”、“重试已失败邮件的队列”及“正在排队等待稍后传递的邮件”。

2. 禁用出站邮件

通过“禁用出站邮件”选项，可以禁用来自所有 SMTP 队列的出站邮件。例如，当组织中有病毒发作时，禁用出站邮件会很有用。

操作方法是在如图 6-207 所示的队列查看器中，单击【禁用出站邮件】按钮，在弹出的确认对话框中单击【是(Y)】按钮即可。



注意

“禁用出站邮件”选项不会禁用 MTA 或系统队列。系统队列是每个协议的默认队列，只有当执行某些必要的路由任务（如内容转换和地址解析）时，这些队列中才会存放邮件。如果在更长的一段时间内在系统队列中找到邮件，则意味着在 Exchange 组织中的某处有一项或多项基本路由功能失败。有关处理队列中邮件堆积的详细信息，请参阅本节后面的“使用 SMTP 队列排除邮件流故障”和“使用 X.400 (MTA) 队列排除邮件流故障”等部分。

如果要阻止特定远程队列中的出站邮件，而不是禁用所有 SMTP 队列，可以冻结该特定队列中的邮件。

3. 冻结特定队列中的所有邮件

冻结特定队列中的所有邮件的方法是在队列查看器要冻结的队列上单击鼠标右键，然后在弹出的快捷菜单中选择【冻结】命令，这时在队列查看器的相应队列上的“状态”列立即显示“已冻结”状态。

要撤销原来已冻结的队列，只需再在相应队列上单击鼠标右键，在弹出的快捷菜单中选择【撤销冻结】命令即可。【撤销冻结】菜单选项只在已是冻结状态的队列上才有。

4. 查找邮件

可以使用“查找邮件”选项并通过指定搜索条件（如发件人或收件人）或邮件状态（如“冻结”）来搜索邮件。还可以指定搜索应返回的邮件数。Exchange Server 2003 中的“查找邮件”与 Exchange 2000 中的“枚举邮件”选项类似。

如要按特定发件人（或收件人）搜索邮件，则可在队列查看器中单击【查找邮件】按钮，打开如图 6-209 所示的对话框。再单击【发件人】（或【收件人】）按钮，通过键入名称或使用搜索条件即可进行搜索。

如要指定搜索应返回的邮件数，可在如图 6-209 所示的对话框“将在搜索中列出的邮件数”下拉列表框中选择一个值，再单击【开始查找】按钮即可。

如要搜索特定状态的邮件，可在如图 6-209 所示的对话框“显示下列状态的邮件”下拉

432 网管员必读——网络应用（第2版）

列表中选择以下可能的选项。

- 所有邮件：该选项显示列表中的所有邮件，不管邮件的状态如何。
- 冻结：此选项显示处于冻结状态的邮件。除了冻结特定队列中的所有邮件外，还可以冻结单个邮件。如果队列中的单个邮件或几个邮件被冻结，那么其他邮件仍然能够流入或流出该队列，并非整个队列都被冻结。
- 重试：此选项显示正在等待下一次传递尝试的邮件。处于重试状态的邮件已经经历了一次或多次传递尝试失败。

以上查找搜索的结果都将显示在“搜索结果”列表中。

5. 使用 SMTP 队列排除邮件流故障

邮件分类和传递期间，所有邮件都要通过 SMTP 虚拟服务器的 SMTP 队列发送。如果在此过程中的任意点上邮件传递出现问题，邮件将留在出现问题时所在的队列中，直到问题解决。使用 SMTP 队列可以找到邮件流出现问题的可能原因。如果某个队列处于“重试”状态，请在队列查看器中选择该队列，并检查该队列的属性以确定原因。例如，如果队列属性显示类似“发生 SMTP 错误”这样的消息，应检查服务器的事件日志以找到任何 SMTP 错误。如果日志中没有事件，应提高 SMTP 日志记录级别，方法是：在 Exchange 服务器上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，在打开的对话框中选择“诊断日志记录”选项卡，如图 6-210 所示。选择“MSExchangeTransport”选项，在其中就可以查看各方面的邮件传输日志记录。

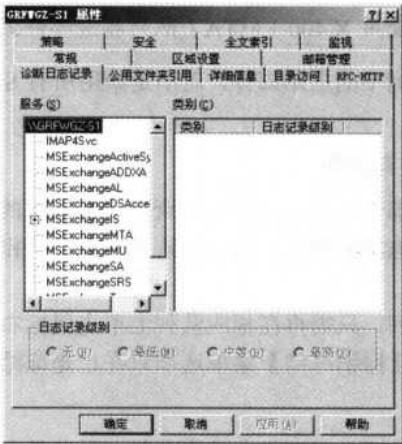


图 6-210 服务器属性对话框“诊断日志记录”选项卡

列表中各服务基本描述如下。

- IMAP4Svc：此服务可使用户通过 Internet 邮件协议版本 4（IMAP4）访问邮箱和公用文件夹。
- MSADC：如果安装了 Active Directory 连接器，此服务将运行连接协议。
- MSExchangeAL：此服务可使用户通过地址列表确定电子邮件的地址。
- MSExchangeDSAccess：Exchange 可通过此服务访问 Active Directory。
- MSExchangeIS：通过此服务可访问信息存储。

- MExchangeMTA: X.400 连接器可以通过此服务查看所使用的邮件传输代理 (MTA)。
- MExchangeMU: 此服务将 Exchange 配置信息更改复制到 IIS 元数据库。
- MExchangeSA: 当 Exchange 使用 Windows 2000 Active Directory 存储和共享目录信息时，此计数器便会记录一个条目。
- MExchangeSRS: 当使用站点复制服务在运行 Exchange 2000 或更高版本的计算机和运行 Exchange 5.5 的计算机之间进行复制时，此计数器便会记录一个条目。
- MExchangeTransport: 当使用简单邮件传输协议 (SMTP) 路由邮件时，此计数器便会记录一个条目。
- POP3Svc: 当使用邮局协议版本 3 (POP3) 访问电子邮件时，此计数器便会记录一个条目。

6.11.5 配置 SMTP 的诊断日志记录

要确定传输问题的原因，可以查看与 MExchangeTransport 有关的事件。如果 Exchange 邮件流出现问题，应立即提高与 MExchangeTransport 有关的日志记录级别。日志记录级别控制在应用程序日志中记录的数据量。记录的事件越多，应用程序日志中与传输有关的事件就越多。因此，可以更好地确定邮件流出现问题的原因。SMTP 日志文件位于 Exchsrvr\Server_name.log 文件夹中。

特定路由和传输组件出现的问题可能导致邮件在队列中堆积，这一点在本节前面介绍的“使用 SMTP 队列排除邮件流故障”主题中已进行了讨论。如果特定队列出现问题，应提高影响队列的组件的日志记录级别。

下面介绍如何修改与 MExchangeTransport 有关的诊断日志记录。

1. 修改 MExchangeTransport 的日志记录设置

(1) 在如图 6-210 所示的“诊断日志记录”选项卡“服务”窗口中选择“MExchangeTransport”选项。

(2) 在“类别”窗口中选择要配置其日志记录级别的类别。

- 要排除路由问题，请选择“路由引擎/服务”选项。如果邮件在“等待路由的邮件”SMTP 队列中堆积，应提高该组件的日志记录级别。
- 要解决 Active Directory 中的地址解析问题、通信组列表展开问题或其他分类程序问题，请选择“分类程序”选项。如果邮件在“等待路由的邮件”SMTP 队列中堆积，应提高该组件的日志记录级别。
- 要解决通过连接管理器的拨号和虚拟专用网连接的问题，请选择“连接管理器”选项，然后提高该组件的日志记录级别。
- 要解决排队引擎的问题，请选择“排队引擎”选项。如果邮件流出现问题，并且邮件未在任何队列中堆积，应提高该组件的日志记录级别。
- 要解决 Exchange 存储驱动器出现的问题，请选择“Exchange 存储驱动器”选项。如果邮件在本地传递 SMTP 队列、X.400 队列中堆积，或者在接收来自 Exchange 5.x 服务器或其他邮件系统的邮件时出现问题，应提高该组件的日志记录级别。

434 网管员必读——网络应用（第2版）

- 要解决一般的 SMTP 问题，请选择“SMTP 协议”选项。如果邮件在“远程传递”SMTP 队列中堆积，应提高该组件的日志记录级别，以确定是否是由于 SMTP 错误而导致了该瓶颈。
- 要解决 NTFS 存储驱动器出现的问题，请选择“NTFS 存储驱动器”选项。如果邮件在本地传递 SMTP 队列中堆积，应提高该类别的日志记录级别。

（3）在“日志记录级别”栏中对应选择“无”、“最小”、“中等”或“最大”单选项。若要进行故障排除，请选择“最大”单选项。



警告

如果提高 Exchange 服务的日志记录级别，性能可能会有所下降。建议用户增加应用程序日志的大小，以包含所有产生的数据。如果不增加应用程序日志的大小，将会频繁收到应用程序日志已满的提醒消息。

2. 启用调试级别日志记录

如果遇到邮件流问题，并且想要查看所有事件，可以修改注册表项，以便将日志记录设置为调试级别，这是最高级别（第7级）。

在调试级别启用日志记录的方法如下。

（1）执行【开始】→【运行】菜单操作，在打开的“运行”窗口中输入 regedt32 命令，按回车键，启动注册表编辑器。

（2）在注册表编辑器中，找到并单击下列注册表项：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeTransport\Diagnostics\SMTPProtocol

双击打开配置对话框，将值设置为 7，单击【确定】按钮即可。

第 7 章 企业即时通信系统

近几年来，即时通信发展非常迅速，因为它为人们提供了另一种更加快捷、更加直接、更加有效（相对于电子邮件通信和电话通信来说）的通信方式。当然最早的即时通信是在公用的互联网上进行的，如人们最早乃至现在都一直使用的 QQ、MSN、ICQ 之类的通信系统。这类即时通信系统不仅可以实现即时聊天，还可以互发文件（相当于文件共享），召开多人会议等许多非常实用的功能。特别是 QQ 群之类的功能，更是得到了许多商业用户的追捧。

随着局域网中的网络应用普及和多样化，加上现在的公司规模也越来越大，集团公司也是越来越多，基于局域网平台的即时通信应用需求也就越来越旺盛，在这种应用需求背景下，基于局域网平台下的即时通信应用也随之兴起，并迅速发展起来。相对于互联网平台下的即时通信系统来说，局域网平台下的即时通信系统可以确保通信更加安全、更有针对性，管理也更加方便（因为服务器是用户自己管理的，而不再是腾讯公司管理的）。

本章要向大家介绍的是在即时通信行业中处于领先地位的深圳腾讯公司的企业 QQ 最新版本 RTX 2006 企业即时通信系统的配置方法。

本章重点

- RTX 2006 的安全技术
- RTX 2006 的服务器配置
- RTX 2006 系统组织架构的部署
- RTX 2006 用户账户创建
- RTX 2006 角色创建与权限配置
- RTX 2006 客户端的个人配置
- RTX 2006 客户端联系人的添加与会话

7.1 即时通信基础

随着互联网的普及和发展，即时通信（Instant Messaging）已经成为人们交流的重要手段。人手一个甚至多个 QQ 号码的情况随处可见，即使通信工具在人们实际的工作、生活和娱乐中发挥着非常积极的作用。利用通信工具不仅可以扩大人们的交友圈子，而且还节省了大量的通信费用。

随着局域网应用的不断普及，基于局域网的即时通信需求也越来越旺盛，所以近几年，这方面的企业即时通信软件系统也不断涌现，其中最经典的要数深圳腾讯公司的企业 QQ（BQQ），后改版为 RTX。

7.1.1 腾讯 RTX 简介

腾讯公司作为国内及亚洲最大的即时通信供应商，利用在个人即时通信市场积累的产品开发经验及市场运营经验，为国内广大的企业用户提供适合中国国情的商用即时通信软件。原有的 QQ 品牌，带有娱乐交友色彩，并不太适用于企业市场；针对商务人士和企业用户的需要，腾讯推出了 RTX（腾讯通）这个新的产品品牌，以更好地服务广大企业用户。

RTX（腾讯通）是腾讯公司的核心技术品牌，同时作为腾讯商业实时应用的品牌。RTX 的前身是 BQQ（企业 QQ），在将 BQQ 更名为 RTX 之后，更突出了腾讯公司在企业即时通信产品方面的定位。

RTX（腾讯通）是腾讯公司推出的企业级即时通信平台。该平台定位于降低企业通信费用，增强企业内部沟通能力，改善企业与客户之间的沟通渠道，创造新兴的企业沟通文化，提高企业生产力。RTX 平台的主要功能，包括企业内部实时信息交互、音视频交流、企业短信中心、自动存档主题讨论等。RTX 平台具有很高的实用性、易用性和可管理性。除了底层采用 128 位对称加密技术之外，在实际应用中，RTX 可以通过员工实名制、记录交互信息等措施，确保企业应用的通信安全。同时，腾讯公司为所有的 RTX 用户提供企业级的信息服务，主要包括企业黄页、企业间协作、网络 IP 电话、集团短信，以及企业与网络消费者实时沟通等服务。

RTX 包括服务器端和客户端软件，可在企业本地自建服务器，迅速搭建企业的内部即时通信平台。同时，RTX 提供二次开发接口，支持第三方在 RTX 上进行二次开发。

目前最新的版本为 RTX2006，可在 RTX 主页 <http://rtx.tencent.com/rtx/download/index.shtml> 上下载试用版。总体来说，RTX2006 与上一版本 RTX2005 在技术上没有太大变动，只是在服务器程序结构上有些小的变化，如 RTX2006 的 RTX 管理器把前 RTX2005 版本的用户管理器、服务管理器、应用管理器整合在一起，只有一个 RTX 管理器入口。具体界面的改动将在本章后面体现。RTX2006 的体系结构如图 7-1 所示。

RTX 系统的软硬件部署，主要包括 3 个部分：RTX 用户工作台（安装 RTXClient）、RTX 服务器（安装 RTX 各类服务）、数据/文件服务器（安装数据库软件/文件系统）。其中，在实际应用中，RTX 服务器与数据/文件服务器可以根据实际情况整合为一台服务器。另外，整个系统通过应用网关——RTX_Gateway 与 Internet 连接，所以，网关的服务器与应用服务器

为同一台服务器。RTX2006 应用的基本网络结构如图 7-2 所示。

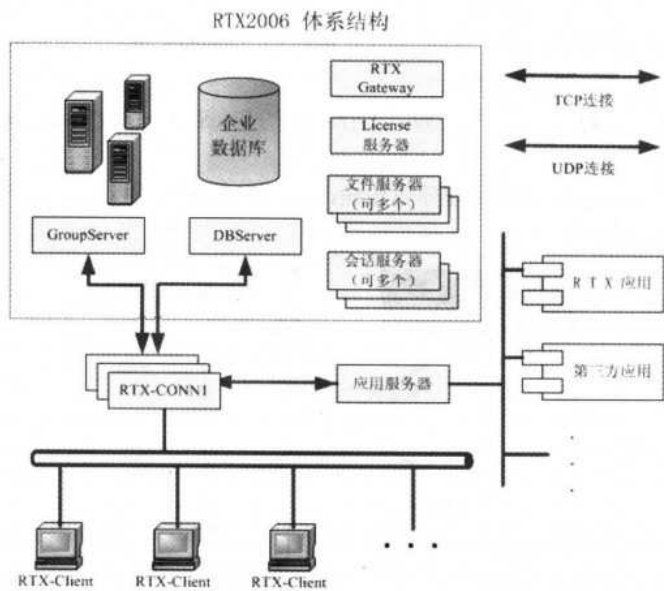


图 7-1 RTX2006 体系结构

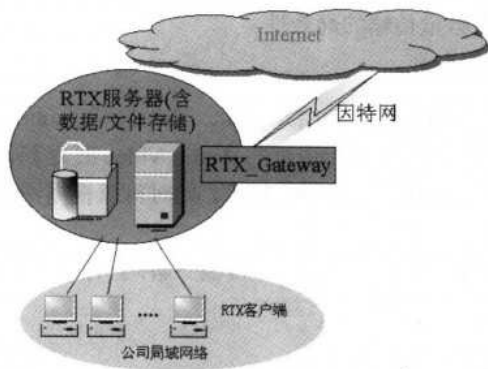


图 7-2 RTX2006 应用的基本网络结构

7.1.2 RTX2006 的主要特性

RTX 自诞生至今也经历了几个版本，RTX2006 是目前最新的版本。在前面已介绍 RTX2006 与 RTX2005 相比，基本上没什么区别，所以 RTX2006 的主要特性与 RTX2005 差不多，主要体现在以下几个方面。

1. 高效的数据传输机制

RTX 系统除了即时通信的常用功能之外，还有会议、讨论组等功能。RTX 系统的通信方式不是只在 RTXClient (RTX 客户端) 与 RTXServer (RTX 服务器端) 的单一 TCP 或 UDP

连接上进行通信，这其中还有 File-Storage（文件存储服务，即 FileServer）的参与。

RTX 通信数据按字节大小和应用上的区别，可以走两种途径。

- 小块数据（小于 4KB），走的是吞吐量较小、持续时间相对较长的 RTX Client 与 RTXServer 之间的轻总线。
- 大型数据（文件），通过与高效、大吞吐量的 FileServer 或者 SessionServer 建立的重总线进行中转发送。

以上这两种途径可以让数据合理分包传输，最大限度地利用网络带宽，提高传输速率。

原理示例如图 7-3 所示。

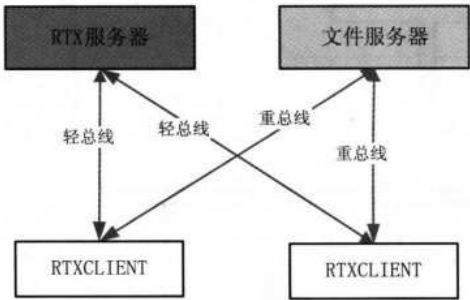


图 7-3 RTX 的两种数据通信途径

另外，在进行语音和视频数据传递的时候，一般采用的是 UDP 方式进行数据传输，充分发挥了 UDP 协议的大数据量传输的高效性。

2. 先进的多媒体技术应用

RTX 使用了业界先进的视频和语音引擎技术，其中包括 Audio/Video（音/视频）的直接交流。在技术上，RTX 系统采用了业界先进的 Audio/Video 处理和传播技术，传输通道上采用了当前互联网上广泛应用的 P2P 先进网络技术，同时可以根据网络带宽情况进行自适应调节，确保最佳的表现效果。

Audio 应用的基本过程是：采样→编码→传输→解码→播放。其中，Audio 编码技术主要分为三类。

1) 波形编码

力图使重建语音的波形保持原始语音的波形形状，如 PCM 和 ADPCM（G.711、G.721、G.722、G.723、G.726 和 G.727）。

2) 参数编码

通过提取、编码语音的特征参数，保持重建语音的可懂度，如 LPC-10e 等（G.723.1）。

3) 混合编码

结合了上述两种方法的优点，能重构高质量的语音，如矢量和激励线性预测、码激励线性预测（CELP）等，如 G.728、G.729 和 GIPS。

在 RTX 系统中，Audio 采用了业界先进的 GIPS 编码技术，保证了音频在采集后的快速、准确、高效的编码及最佳的表现效果。

Video 应用的基本过程与 Audio 类似，也是：采样→编码→传输→解码→播放。

其中，Video 编码技术主要分为三类：第一类，考虑到图像信源的统计特性采用的预测

编码方法、变换编码方法、矢量量化编码方法、子带一小波编码方法及神经网络编码方法等；第二类，考虑到视觉特性采用的基于方向滤波的图像编码方法、基于图像轮廓/纹理的编码方法；第三类，考虑到图像传递的景物特征采用的分形编码、基于模块的编码方法。

在 IP 视频通信应用中，编码方法的选择不但要考虑到压缩比、信噪比，还要考虑到算法的复杂性。太复杂的编码算法可能会产生较高的压缩比，但也会带来较大的计算开销，软件实现时会影响通信的实时性。目前，在众多视频编码算法中，影响最大并被广泛应用的算法是 MPEG 和 H.26x 系列。

在 RTX 系统中，Video 采用的是在 H264 基础上自行研究的增强编码方法。H264 编码就是 MPEG4 与 H26L 的有机结合，是 ITU 和 IETF 后续统一的视频标准。

3. 稳定高效的数据/文件存储

RTX 系统服务器端采用了 Access 数据库作为数据存储方式，利用 ODBC 访问技术，采用最优的系统分析方法指导数据库表的设计，充分发挥了 Access 数据库小巧、稳定、高效、灵活的特点。

另外，当交互的数据流比较大的时候，RTX 系统采用文件的方式存储数据流，利用操作系统提供的文件管理功能，灵活地避免了 Access 数据库日渐庞大所带来的效率降低。在以后的升级版本中，RTX 系统将引入腾讯公司自身开发的一套更灵活、简便、稳定的文件存储系统。

7.1.3 RTX 2006 的安全技术

RTX 系统在数据通信中，采用 128 位消息加密机制，确保信息在各个通路之间中的传输安全。同时，配合严谨而灵活的用户权限机制，最大程度上解决了企业应用中的安全隐患问题，具体表现如下。

1. 数据加密打包传输（128 位标准对称加密算法）

RTX 系统中各个模块之间、各个插件之间的数据通信，都采用的是 TCP 协议与 UDP 协议相结合的传输方式，增强了通信方式的灵活性。同时，为了避免数据的明文传递，系统采用了多种 128 位标准对称加密算法进行数据加密，支持 IDEA、TEA、THEA 等多种算法以及在算法之间的轮换应用。这样，即时通信信息、文件、讨论组信息等可能因为明文而造成的网络传输安全隐患，在 RTX 系统中得以合理消除。

在实际应用中，涉及登录信息、权限变更等关键数据，都是采用数据加密并从服务器转行 TCP 协议的方式；而非关键的数据，类似语音流、视频流等，才是通过 UDP 协议实现高效的传送。UDP 协议在传输中是可以被伪装的，要实现高安全性，需要通过若干次“握手”通信及 SessionKey 的方式来保证，而这样的保证，又大大降低了它的高效性，因此，可以应用 UDP 协议来进行非关键数据的高效传输。

2. 严谨的用户权限机制

在企业用户应用 RTX 系统的时候，系统管理员、普通客户端用户、信息服务部门管理员等，不同的角色在系统中有不同的用户权限。RTX 系统采用了严谨而又非常灵活的用户权限机制，以求能够合理地搭建企业实际应用的权限框架。

RTX 的用户权限机制分为两方面的内容，即“身份验证”和“访问控制”。

440 网管员必读——网络应用（第2版）

- 身份验证：可以确认客户身份的唯一性，而不是其他假冒的身份。
- 访问控制：对通过身份验证的客户进行服务器端访问权限控制。主要是指对服务器对象的访问权限，比如信息服务中文件的读写、会议室的建立、讨论组的发起等。

权限模型自动根据不同用户的不同身份验证资料，在系统的各个应用层面，赋予用户不同的访问控制权限（访问令牌）。不同的用户，获得若干不同的访问令牌，以不同的访问令牌，享有各个不同服务的访问权限。

权限模块是作为一种服务存在的，为各种服务器对象提供权限的服务，主要提供 RTX 用户的访问令牌的管理，服务器对象的访问控制的管理等。

3. 签名和令牌

Kxxx：一般代表某种用于加密的密钥。密钥的类型由 xxx 表示。例如 Ks 表示 Session Key。

Kxxx (a,b,c...)：一般代表用密钥加密的内容，括号内的内容字段用逗号分隔。例如 Ks (dwUin,dwIP,dwPort) 表示用 SessionKey 加密内容为 Uin、IP、Port 的信息。

Signature (Buin,Cuin)：一般代表用户的签名。例如 Signature (72800008, 1001)。

SS Key：Server 体系内部约定的 Key，Client 程序是绝对不应该知道的，SS Key 只用于 Server 体系内部用于分布式身份认证使用。

每个客户端登录 RTX Server 后，会从 RTXServer 处获得一个二进制的加密信息，称之为签名。签名中含有用户的标志信息以及存活期，可以作为访问其他 RTX 服务时的身份标识。签名的内部信息包含：用户的 BUin、CUin、服务器当前时间，以及签名的存活期。

签名是采用 RTX 服务系统内部约定的一个密钥（Kss）进行加密的，只有知道 Kss 的服务程序才能解开。

上面所述的 dwBuin 表示企业号；dwCUin 表示分机号；dwTime 表示当前的服务器时间；dwLifeTime 表示签名的有效时间（存活期），一般为 24 小时。

客户端在登录其他服务器（例如 File Server, SessionServer）之前，需要到 RTXServer 取到一个其他服务器的访问令牌（Access Token）。

第三方服务器的认证步骤如下。

- (1) Client 向 RTX Server 取第三方服务器的验证串。
- (2) RTX Server 返回 Kcs、AT (Buin,Cuin)。Kcs 是与第三方服务器进行双向认证的“握手”Key。
- (3) Client 程序将 AT 及用 Kcs 加密的相关协议信息发到第三方服务。
- (4) 第三方服务器用 Kss 解开 AT，如果解密失败，表示 Client 身份不正确。如果解密成功，则取出 AT 里的 Kcs，处理完相应信息后，用 Kcs 加密要返回的信息，其中包括后续 C/S 通信的 Session Key, Ks。
- (5) 第三方服务器将用 Kcs 加密的信息返回给客户端。客户端用 Kcs 进行解密，如果解密失败，表示服务器身份不正确。如果解密成功，取出新的 Ks 作为后续与第三方服务器进行通信的密钥。

7.1.4 RTX2006 系统的基本部署思路

继承本书的一贯风格，在具体介绍各软件系统配置之前，先理清一下整个应用系统的部

署和配置思路，这样可以使应用系统部署更加顺利、更加完善。不过，对于这样一个涉及到所有员工的应用系统，在正式在企业中全面使用之前，先进行一些试点，以积累应用和管理经验。下面是建议的该应用系统总体部署流程。

1. RTX2006 应用系统总体部署流程

1) 了解企业各部门对即时通信的需求和接受程度

信息系统的建设一般由 IT 部门和公司领导牵头规划，信息系统要真正发挥作用，还需要得到企业最终用户的认可和支持，所以在进行部署之前，需要先听听最终用户的意见，主要有几方面。

- 用户在日常办公中，企业员工对交流和信息的即时性要求。
- 咨询、了解用户对 RTX 主要功能的需求和看法，了解用户最需要的功能有哪些，哪些功能可以帮助用户解决哪方面的实际问题，从而了解到在部署中哪些功能是需要重点支持的。

RTX 主要功能包括：实时交流（消息、语音/视频、图片）、文件传送、语音视频、企业短信中心（短信单发群发、手机直接回复、手机短信查询通信录等）。

建议对用户的了解、咨询需要包括公司的主要职能部门，包括管理层，以及生产、技术、管理、市场等部门，并且建议针对部门的负责人或主管以上人员，并以面谈方式进行。对于用户的各种想法和意见，应该以书面方式记录下来，作为部署的重要参考。

2) 部门内部试用，积累推广经验

为了 RTX 在企业的顺利推广，建议在企业各部门部署、推广 RTX 之前，先在 IT 部门内部进行试用，重点针对之前调查中用户比较关心的一些功能，并收集试用过程中的用户反馈。

为了全面积累实际的应用经验，部门内部试用最好不少于 15 人，如果不足 15 人，可考虑与其他部门联合试用（对于少于 50 人的企业，如果对即时通信能较好理解，可考虑直接全面部署，不需要局部试用）。试用过程中，须要求参与人员在上班时间都登录 RTX 服务器。

试用过程中，记录下容易让用户困惑的功能和操作，并整理成 FAQ 文档。局部试用时间一般在控制在周以内，如果对 RTX 主要功能未能熟练掌握，可考虑延长试用时间。正常情况下，可考虑对部门内试用进行阶段性总结，为推广做准备。

3) 制订 RTX 推广方案，争取公司领导支持

对于不同的企业，需要有针对性的推广方案，通过客观评估企业内部的需求和接收程度，以及推广投入估算，制定出合理、可行的推广计划，争取公司领导支持，确保推广顺利进行。

推广方案中，需要着重考虑以下几方面。

- 即时通信对企业的好处，解决了哪些问题。
- 用户对 RTX 主要功能的需求和接受情况。
- 局部试用情况的总结。
- 推广所需要的配合，包括安装部署、技术支持、用户培训、行政支持等。
- 如果企业较大规模或有多个分支机构，还需要考虑分期推广计划。

从企业规模来看，一般对于少于 50 人的企业，可考虑进行一次性推广的方式；对于 200 人左右的企业，可考虑先进行内部局部试用，再全面推广的方式；对于超过 500 人的企业，在内部局部试用之后，可考虑进行分期推广的方式；对于有分支机构的企业，先实施总部，再分期部署分支机构。

442 网管员必读——网络应用（第2版）

从企业内部对即时通信的需求和接收程度来看，如果能较好理解即时通信功能，可考虑较快速地全面推广。如果未能很好理解，一方面可通过用户培训，让用户更好地了解即时通信为企业带来的好处；另一方面，可通过先树立用户较容易接收的典型应用，加强用户对即时通信功能的认识，例如短信、语音视频等。

顺利地推广离不开领导的支持，对于公司领导，一方面可以通过一些典型应用让领导体验即时通信为办公带来的便利，另一方面，通过局部试用报告和企业员工对即时通信的需求可以向领导说明企业推广的必要性。同时，还需要一份合理、可行的推广计划让领导放心。

对于企业较大规模或多分支结构，强烈建议成立 RTX 推广小组，由企业高层挂帅，将极大提供推广的力度和减少可能出现的一些障碍。

4) 结合培训，有计划地在公司各部门进行推广，并做好技术支持工作

在推广方案完成后，需要有计划地在公司各部门采取以下方式进行推广。

- 推广与培训相结合。如果公司员工较多，可按部分对用户进行操作培训，并在操作培训之后，着手该部门的推广使用。
- 培训前，需要准备好相关资料、PPT（课件）和实验环境。
- 开展有针对性的培训，对于不同的部门，由于对计算机的掌握程度的差异，培训时，需根据不同部门开展有针对性的培训，尤其是对前期调查中有较明显需求的功能重点介绍。
- 对公司领导、人力资源部、行政部重点培训将有利于 RTX 在各部门推广的顺利进行。

在推广中，需要做好技术支持准备，需要让有需要的人能及时通过电话或邮件得到帮助。

5) 部署完毕后，考虑 RTX 是否需要和现有信息系统集成，进一步增效

RTX 不仅有利于日常办公的即时沟通，实时的信息传递能让企业信息系统更加高效地运作，例如通过与 RTX 集成，可以实现通过手机短信查询库存，可以实现来文的即时提醒。

在 RTX 在企业运行一段时间（建议一个月以上），可以考虑是否通过 RTX 所提供的二次开发接口，将已有的信息系统和 RTX 联系起来，使信息能够更加实时地传递。也可以通过访问 <http://rtx.tencent.com> 网站获得更多插件功能。

2. RTX2006 应用系统配置思路

安装、配置 RTX2006 系统的基本思路比较简单，具体如下。

(1) 准备好 RTX 服务器 IP 地址，如果 RTX 要与集团公司分支机构 RTX 服务器互连，则还要准备好相应的网络连接方式。

(2) 安装好 RTX 服务器和客户端软件，如有必要，还可安装自带的 SDK 程序。

如果仅用于本地局域网内部，则 RTX 服务器的安装在网络方面就没有什么特别要求了，只需要有一个固定的 IP 地址；如果本地 RTX 服务器还要与远程分支公司的 RTX 服务器互连，则还需要配置 RTX 服务器的互联网连接，当然既可以是固定 IP 地址+因特网域名方式，也可以是动态 IP 地址+域名方式。如果是动态 IP，则还需要采用本书前面介绍的动态域名解析服务。

RTX 服务器安装的硬件要求是磁盘建议 5GB 以上剩余空间；256MB 以上内存；Pentium 4 系列或以上的 CPU，如果是在大型网络中，则建议使用专业的双处理器服务器。软件系统要求是微软 Windows 2000 Server 或以上。

因为具体的软件安装过程都非常简单，所以本章不具体介绍安装步骤。只是在安装

RTX2006 服务器系统时，会弹出一个如图 7-4 所示的对话框，要求配置超级管理员密码（以前版本没有这个），这个密码一定要记住了，否则进入不了服务器系统。

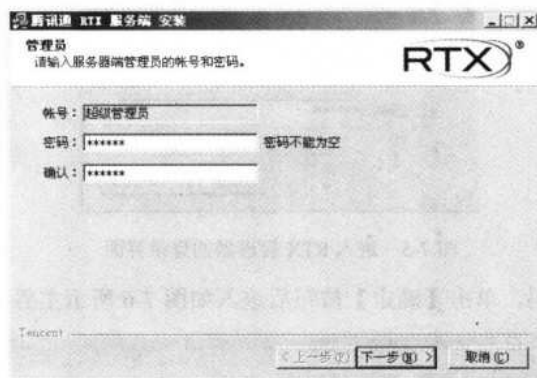


图 7-4 配置超级管理员密码对话框

（3）配置 RTX 管理器。

通过 RTX 管理器配置各种 RTX 服务器，如主服务器、数据库服务器、应用服务器和 HTTP 服务器（只是在需要通过互联网与远程 RTX 服务器互连时才需要配置），使它们均能正常工作。

RTX 管理器的具体配置步骤参见本章 7.2 的内容。

（4）在 RTX2006 中配置企业 RTX 系统组织架构。

RTX 即时通信应用系统的建设首先要配置的是应用系统的组织架构。RTX 组织架构的设置通常是按部门进行组织的，当然，在部门下也可以有子部门和最终用户。其实这一点与 Windows 系统下的组有些类似，组中可以有用户和子组。

组织架构中的部门可以指派不同的权限，它作用于其下的子部门和最终用户。

具体配置方法参见本章 7.3 的内容。

（5）添加与管理用户。

组织架构设置好后，就可以把最终的用户添加到各个对应的部门中了。

具体添加方法参见本章 7.4 的内容。

7.2 RTX 管理器的设置

RTX 管理器把前 RTX2005 版本的用户管理器、服务管理器、应用管理器整合成一个 RTX 服务管理器，只有一个 RTX 管理器入口。本节首先要介绍的是通过 RTX 管理器来设置 RTX2006 中的各项服务器。具体的设置步骤如下。

（1）执行【开始】→【所有程序】→【腾讯通】→【腾讯通 RTX 管理器】菜单操作，首先打开的是如图 7-5 所示对话框，要求正确输入安装 RTX 服务器端程序时所配置的超级管理员密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-5 进入 RTX 管理器的登录界面

(2) 正确输入密码，单击【确定】按钮后进入如图 7-6 所示主界面。

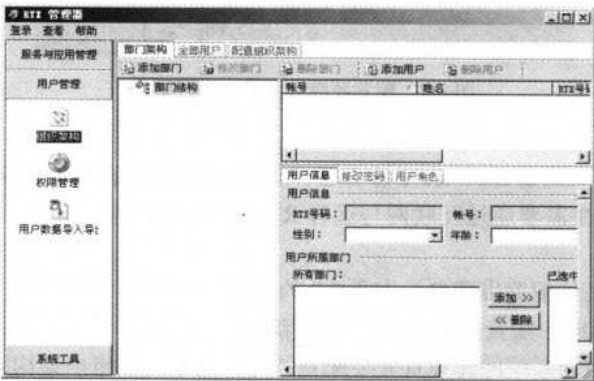


图 7-6 “RTX 管理器”主界面

(3) 在左边导航栏中单击【服务与应用管理】按钮，然后在展开的导航栏中选择“服务管理器”选项，打开如图 7-7 所示设置界面。

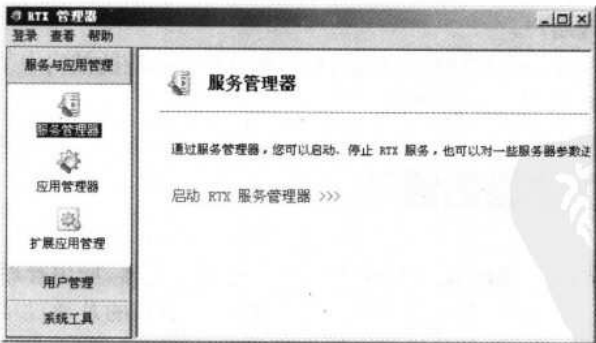


图 7-7 “服务管理器”界面

(4) 单击【启动 RTX 服务管理器】链接，打开如图 7-8 所示对话框。在“服务”列表中包括两个服务选择项：“RTX_SVRMAIN”（RTX 主服务）和“RTX_HTTPServer”。查看这两项服务是否都正常启动，当然，如果不需要与远程 RTX 服务器互连，则“RTX_HTTPServer”服务选项可以不正常工作，但“RTX_SVRMAIN”选项一定要工作正常。查看是否正常工作，

就要看选择对应服务项，在对话框下面的状态栏中是否显示“服务运行正常”。

(5) 除了可以查看和设置“RTX_SVRMAIN”(RTX 主服务)和“RTX_HTTPServer”服务选项外，还可以进一步设置各服务项所有的端口和 IP 地址等选项。其实一般情况下是无须任何另外设置的。方法是在如图 7-8 所示界面中执行【设置】→【基本配置】菜单操作，打开如图 7-9 所示对话框。在“ConnServer 端口设置”栏中可以设置客户端登录 RTX 服务器时所用的端口，“ConnServer 的 TCP 端口”和“ConnServer 的 UDP 端口”两文本框中分别设置服务器为 RTX 客户端提供的连接服务所用的 TCP 和 UDP 端口，通常不要更改默认的 8000 端口的。

在“FileServer 端口设置”栏中的“FileServer 的端口”选项可以设置用户发送和接收文件时所用的端口，通常也不要更改默认的 8003 端口。

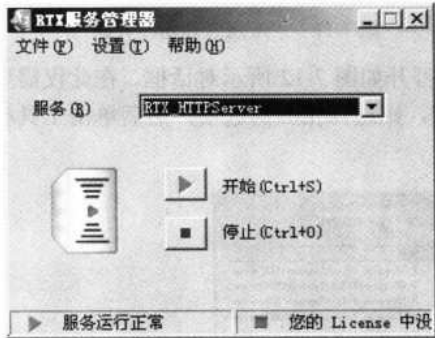


图 7-8 “RTX 服务管理器”对话框

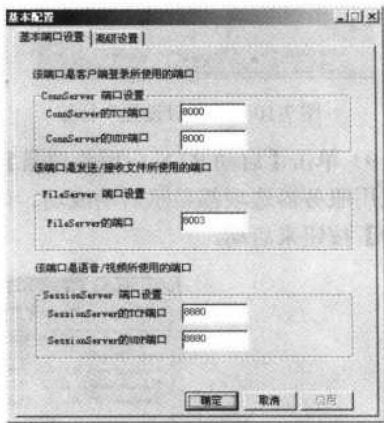


图 7-9 “基本端口设置”标签

在“SessionServer 端口设置”栏中可以设置语音和视频通信时所用的端口，“SessionServer 的 TCP 端口”和“SessionServer 的 UDP 端口”文本框中设置服务器为客户端提供会话服务所用的端口，通常也不要更改默认的 8880 端口的。

(5) 单击“高级设置”标签，打开如图 7-10 所示配置对话框。在“DBServer 配置”栏中可以设置 RTX 连接服务器所需的数据库服务器 IP 地址和所用的 UDP 通信端口。在“DBServer 所在机器的 IP”和“DBServer 的 UDP 端口”两文本框中分别可以设置数据库服务提供主机的 IP 地址和数据库服务的 UDP 端口。数据库服务主机 IP 地址可根据具体情况重新配置，UDP 端口号则最好采用原来的 9000。在 IP 地址设置中如果所有 RTX 服务器都在一台主机中安装，且均在本地局域网中使用，无须与远程 RTX 服务器互连，则可不改变默认的 127.0.0.1 设置，当然最好设置成另外一个静态 IP 地址。

在“GroupServer 配置”栏中可以设置连接服务器与组服务器连接时所用的 IP 地址和 TCP 端口。在“GroupServer 所在机器的 IP”和“GroupServer 的 TCP 端口”两文本框中分别可以配置工作组服务主机的 IP 地址和所用的 TCP 端口。同样，主机 IP 地址可根据具体情况重新设置，而所用的 TCP 端口则最好仍保持为 9001 不变。

(7) 完成配置后单击【确定】按钮退出即可生效。至于在【设置】菜单中的其他设置选项，在此不作介绍，一般情况下，也不用更改设置。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(8) 再回到如图 7-7 所示界面。在导航栏中选择“应用管理器”选项，打开的界面如图 7-11 所示。

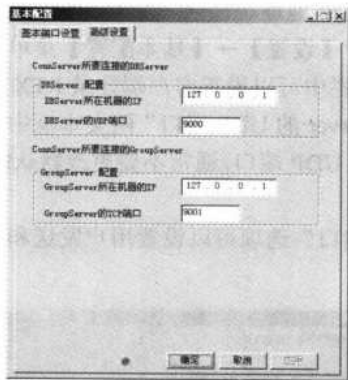


图 7-10 “高级设置”标签

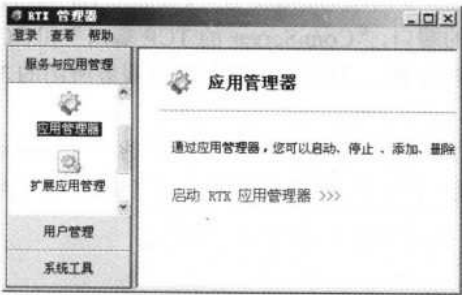


图 7-11 “应用管理器”界面

(9) 单击【启动 RTX 应用管理器】链接，打开如图 7-12 所示对话框。在此仅需要确保每个应用服务器选项都显示启动成功。如果没有，则选择相应的选项，然后单击工具栏中的【启动】按钮来启动。

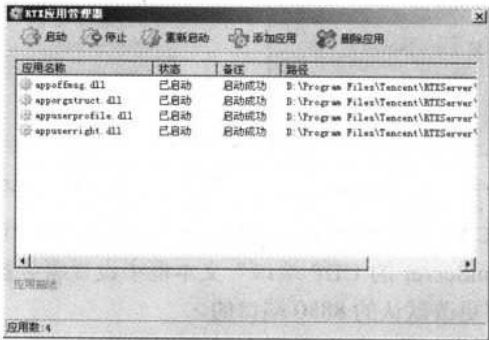


图 7-12 “RTX 应用管理器”对话框

一般情况下，RTX 管理器就只需进行以上设置即可。

7.3 部署组织架构

根据 RTX 系统的设计原则，RTX 客户端用户是不能自动申请 RTX 号码的。系统需要由 RTX 系统管理人员架构企业的部门组织结构，分配 RTX 号码，然后才可以由 RTX 客户端进行登录。所以，首先必须配置好自己单位的组织架构。

7.3.1 添加一级部门

在 RTX2006 中，进入添加一级部门功能的方法如下。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(1) 在如图 7-11 所示界面左边导航栏中单击选择【用户管理】按钮，在展开的导航栏中选择“组织架构”选项，界面如图 7-13 所示。



图 7-13 “RTX 管理器”主界面

(2) 在右边窗口中单击【添加部门】按钮，打开如图 7-14 所示对话框。在这里要在“部门名称”文本框中输入新建的一级部门名称。因为是一级部门，所以在“父部门”下拉列表框中选择“无”选项。然后在“部门位置”栏中根据实际管理级别选择对应选项。然后单击【添加】按钮完成一个新的一级部门创建，可以在同一个对话框中继续添加其他一级部门。

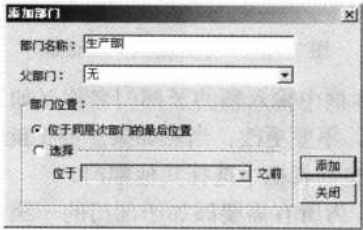


图 7-14 “添加部门”对话框

(3) 用上述同样的方法创建其他一级部门。添加好的一级部门如图 7-15 所示。



图 7-15 添加新部门后的“用户管理器”界面

7.3.2 添加多级部门

RTX 系统支持多级部门的添加，即在部门下添加子部门，以满足企业应用中实际组织架构的需要。进入添加多级部门的方法，类似添加一级部门，需要注意的是，当需要在那个部门下添加子部门的时候，可以在主界面左侧定位到该部门然后打开添加窗口。具体方法如下（以在一级部门“生产部”下添加子部门“插件车间”、“组装车间”和“总装车间”为例进行介绍）。

（1）在如图 7-15 所示界面的中部部门结构窗口中选择“生产部”选项，再直接单击工具栏中的【添加部门】按钮，或者在其上单击鼠标右键，在弹出的快捷菜单中选择【添加部门】命令，可打开如图 7-16 所示对话框。

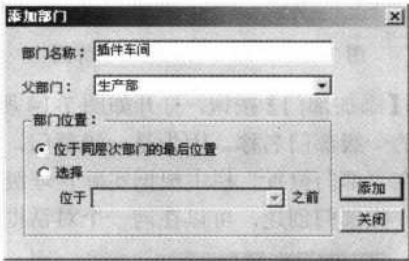


图 7-16 “添加部门”对话框

（2）在“部门名称”文本框中输入新的子部门名称（如“插件车间”），在“父部门”下拉列表框中按系统默认显示，不要更改。当然如果想要把此次添加的子部门放在其他一级部门中，则可在“父部门”下拉列表框中选择其他部门。

（3）用上述同样的方法，为所有需要添加子部门的一级部门添加子部门。添加了子部门后的组织架构界面如图 7-17 所示。

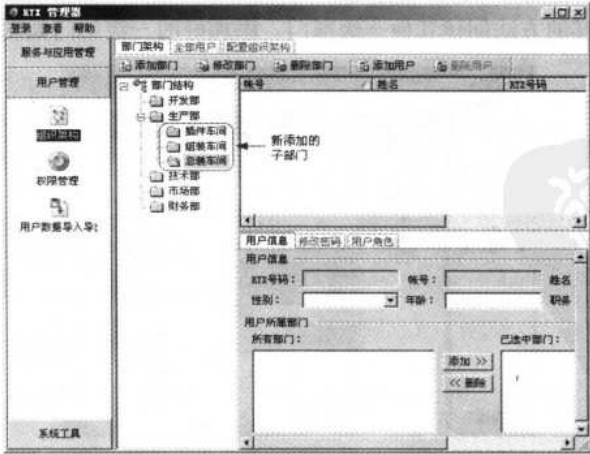


图 7-17 添加了二级部门后的“组织架构”界面

如果在子部门下还可有子部门，则仍按上述方法添加、配置。

如果要修改以上创建的一级部门和多级部门，则可直接在相应的部门上单击鼠标右键，在弹出的快捷菜单中选择【修改部门】命令，打开如图 7-18 所示对话框。在其中可以修改部门名称、调整相应部门的上级部门，以前它与同级部门之间的位置。修改设置后单击【修改】按钮即可完成修改并生效。

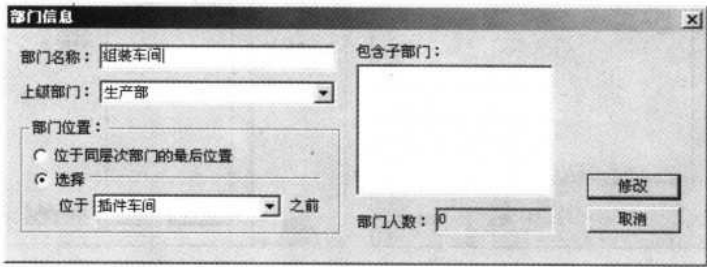


图 7-18 修改部门对话框

7.3.3 新建组织架构

上面两小节介绍的是默认组织架构配置的基本方法，但在配置好了默认组织架构后，如果要再创建新的组织架构（为新的分公司创建），如果新公司的组织架构与原有公司的组织架构相类，则可以充分利用原有的默认组织架构了，经过比较简单的修改、调整即可达到新组织架构创建的目的，而不必重新一一为组织架构创建部门和用户账户。具体方法如下。

（1）在如图 7-17 所示界面中，在中部分窗口中选择“配置组织架构”标签，界面如图 7-19 所示。此时界面中显示的是上面所使用的默认组织架构。

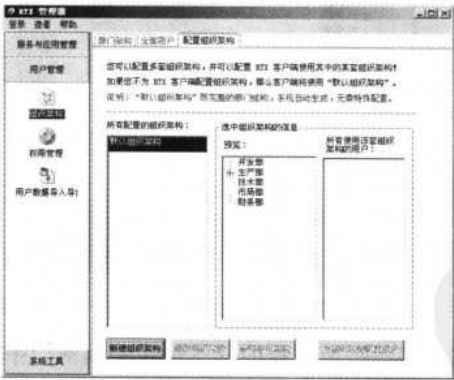


图 7-19 “配置组织架构”标签界面

（2）单击界面底部的【新建组织架构】按钮，打开如图 7-20 所示对话框。在这里的“请输入组织架构的名称”文本框中输入新组织架构的名称；在“选择组织架构包含的部门”列表中根据新组织架构的实际需要，手动选择列表框中所列的默认组织架构中所包括的部门，也可以单击左边的【全部选中】按钮来选中列表中所列的全部部门，也可以单击【全部不选】按钮取消原来的所有选择。然后单击【确定】按钮完成新组织架构的基本设置，新的组织架构配置成功后，在如图 7-19 所示界面中会同时显示所创建的组织架构，如图 7-21 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

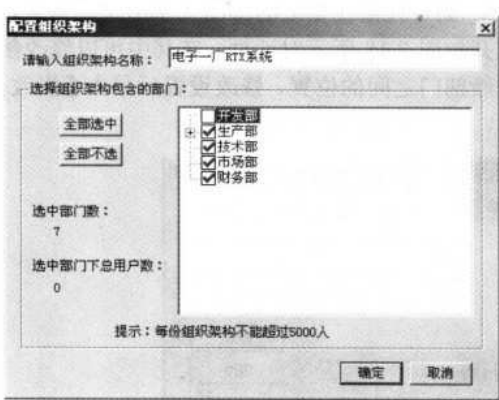


图 7-20 “配置组织架构”对话框

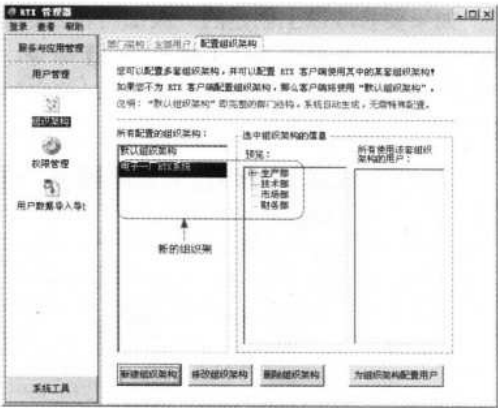


图 7-21 新的组织架构配置好后的
“配置组织架构”标签界面

(3) 组织架构创建好后，还可以向组织架构中添加用户，它也是通过从默认组织架构中导入的。单击【为组织架构配置用户】按钮，打开如图 7-22 所示对话框。在其中的“请选择组织架构”下拉列表框中选择新建的组织架构，然后在“选择使用该套组织架构的用户”列表中选择要从默认组织架构中添加用户的部门。不过，一般情况下是不直接引用原组织中的用户，因为员工都不一样，除非是在同一公司中重新部署组织架构。

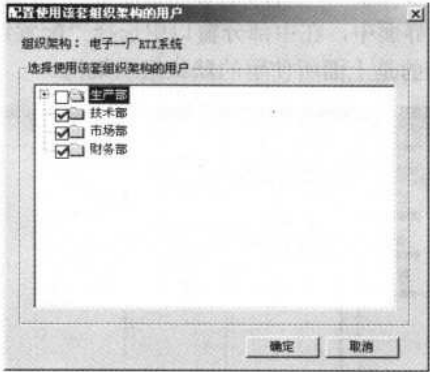


图 7-22 “配置使用该套组织架构的用户”对话框

(4) 单击【确定】按钮即可把所选择的默认组织架构部门中的用户导入到新的组织架构中。要修改组织架构配置，可在如图 7-21 所示对话框底部单击【修改组织架构】按钮，如果要删除组织架构，则可单击底部的【删除组织架构】按钮。

7.4 管理用户信息

RTX 管理员在按照企业实际组织结构，创建了各级部门信息之后，接下来要做的工作，就是将企业中的每位工作人员的账号信息添加到相应的部门中去，以完成企业组织的搭建。

7.4.1 添加单个用户

1. 添加用户

在部门中添加用户的方法有两种，一种是在如图 7-17 所示界面的组织架构中直接选择相应部门，然后单击鼠标右键，在弹出菜单的快捷中选择【添加用户】命令，打开如图 7-23 所示对话框。

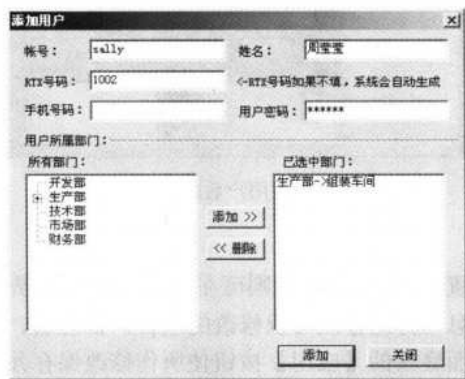


图 7-23 “添加用户”对话框

另一种方法是直接在如图 7-17 所示工具栏中单击【添加用户】按钮，同样会打开如图 7-23 所示对话框。

具体的添加单个用户的方法如下。

(1) 在如图 7-23 所示对话框中，在“账号”文本框中输入用户账户名称（此处必须配置）；在“姓名”文本框中输入相应用户账户的名称（此处也可以不配置）；在“RTX 号码”文本框中输入相应用户分配的 RTX 号码（也可不配置，这样 RTX 程序会自动为用户分配一个 RTX 号码），号码必须在 1 001~200 000 之间，1 000 是 RTX 公共管理号，不能用。在“用户密码”文本框中输入一个用户初始密码（也可不配置，这样用户的初始密码就为空，用户登录后可以自己修改，与 Windows 系统中的用户密码一样）；“手机号码”文本框中可以不配置。

(2) 如图 7-23 所示对话框采用的是第一种打开方式，则下面的“用户所属部门”栏就可以不用配置了（但如果该用户要隶属于多个部门，则也需要按后面介绍的方法添加）；但如果采用的是第二种打开方式，则要把该用户所属的部门从“所有部门”列表中选择所属的部门，然后单击【添加】按钮添加到右边的“已选中部门”列表中。

(3) 添加一个用户后，如图 7-23 所示对话框并不会退出，而清空所有配置项，然后可继续添加其他用户。当所有用户添加完后单击【关闭】按钮退出。



注意

此处配置的用户信息中，“账号”、“RTX 号码”和“姓名”三个属性在 RTX 客户端是不能修改的。另外，同一个用户可以隶属于多个部门，根据实际需要而定，就像 Windows 系统中的用户可以隶属于多个组一样。

如图 7-24 所示是在为“组装车间”添加了三个用户界面并选择相应用户后，在界面的下面针对性地显示相应用户的配置信息。



图 7-24 添加了用户后的部门用户窗口

2. 修改用户信息

如果发现某用户的配置信息需要修改，则可在如图 7-24 所示界面中选择相应部门的相应用户，在下面的“用户信息”标签修改可以修改的项目，如姓名、性别、年龄、职务、所属部门。修改完成后单击界面底部的【应用】按钮使所作修改保存并生效。

如果还要为用户修改密码，则可在如图 7-24 所示下部界面中选择“修改密码”标签，如图 7-25 所示。在其中先为该用户输入新密码，然后单击【修改】按钮即可使修改保存并生效。

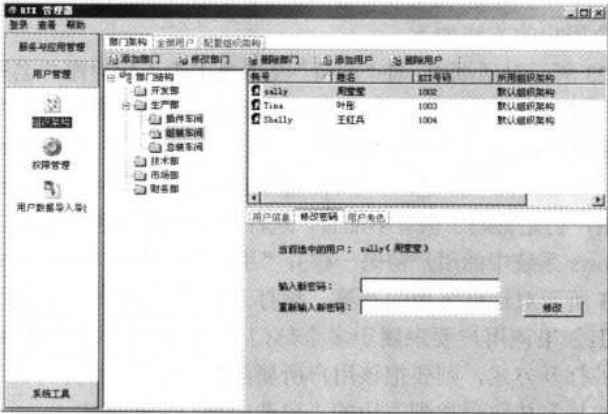


图 7-25 “修改密码”标签界面

3. 删除用户

当需要删除某个用户的时候，以删除“组装车间”的用户“shelly”为例进行介绍。选择该用户，然后单击鼠标右键，在弹出的快捷菜单中选择【删除用户】命令，打开如图 7-26 所示信息提示框，选择“彻底删除用户”复选项，则将此用户删除；选择“只把用户从当前部门删除”复选项，则用户如属于多个部门时，还将存在于其他部门，只是从所选择的部门中删除相应用户。

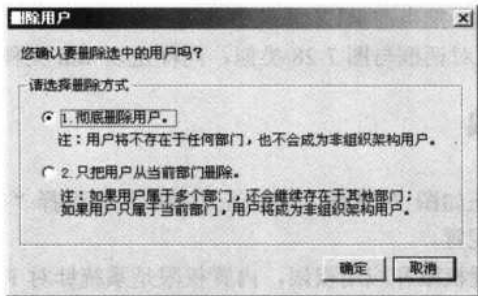


图 7-26 “删除用户”提示框

7.4.2 批量导入用户数据

这一功能是在如图 7-25 所示界面左边导航栏中选择“用户数据导入导出”选项，相应的配置界面如图 7-27 所示。管理员通过该功能，将该版本之前的及 RTX2005 版本之后的 RTX 用户导入到本系统中。

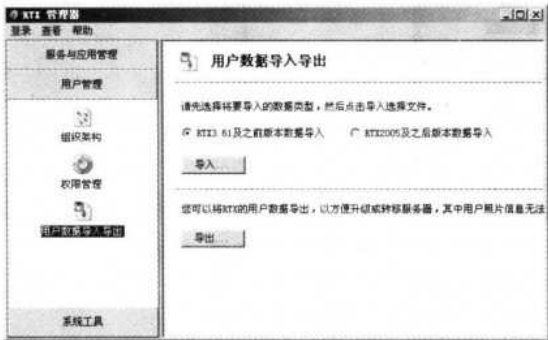


图 7-27 “用户数据导入导出”界面

首先要选择导入的用户数据类型。界面中包括两个单选项：“RTX3.61 及之前版本数据导入”和“RTX2005 及之后版本数据导入”。选择好后单击【导入】按钮后，打开如图 7-28 所示对话框。在其中选择用户数据文件（注意，此处可导入的文件类型只能是 xml 文件），选择好后单击【打开】按钮，用户数据即可导入到本系统。



图 7-28 选择导入数据对话框

454 网管员必读——网络应用（第2版）

顺便说明一下，如果要把当前 RTX 系统中的用户数据导出，则需在如图 7-27 界面中单击【导出】按钮，打开的对话框与图 7-28 类似，同样是以 xml 文件格式保存。

7.4.3 为用户分配权限

RTX 的权限配置可在如图 7-27 所示界面左边导航栏中选择“权限管理”选项，在打开的如图 7-29 所示界面中配置。

RTX 的权限分为内置权限和应用权限，内置权限是系统针对 RTX 自身功能所设置的权限；应用权限是针对所集成的插件应用功能所配置的权限，应用权限用户可在添加插件或应用时自行添加。

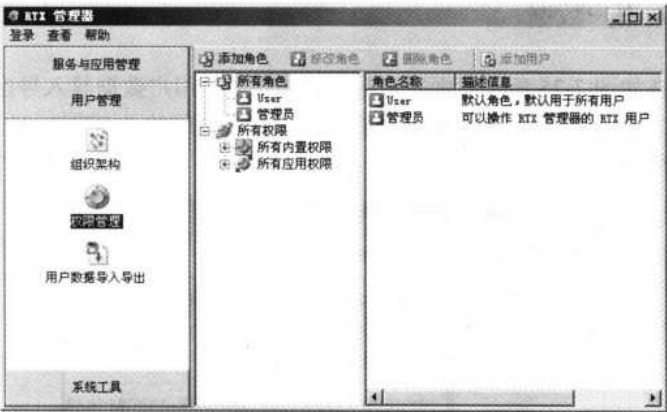


图 7-29 RTX 权限管理界面

1. 角色

用户所具有的权限全部由角色（相当于 Windows 系统中的“组”功能）所实现，在分配权限之前，先必须为每个用户或者部门分配角色。每个角色拥有不同的权限值。系统内置了“user”和“管理员”这两个角色（如图 7-30 所示），并默认所有用户均属于角色“user”。这就相当于 Windows 系统中的“Users”组一样，所以用户在添加之后自动归属于这个组中。

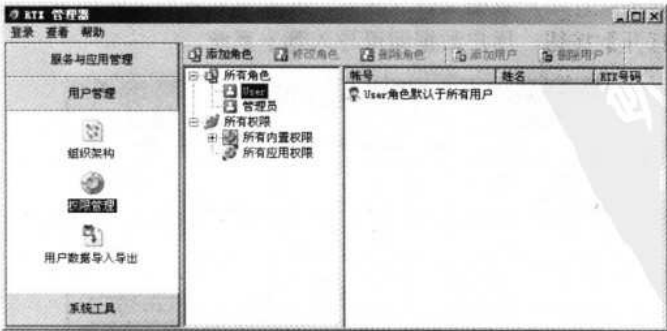


图 7-30 “User”角色界面

User 角色默认所具有的权限值包括以下几方面（参见图 7-31 所示）。

- 发送短信：允许。
- 发起 30 人以上的多人会话：允许。
- 发送大于 3MB 的文件：允许。
- 点对点方式传送文件：允许。
- 传送广播消息：拒绝。
- 远程登录：不允许。

“管理员”角色除了不能指派管理员外，以上所有权限均允许。



图 7-31 “User”角色默认权限

如果要添加新的角色，可在如图 7-31 所示界面中选择“所有角色”选项，单击工具栏中的【添加角色】按钮，打开如图 7-32 所示对话框。在其中的“角色名称”文本框中可以输入角色名称，这个角色名称可以自己定义。在“描述信息”文本框中输入一些角色描述类的信息，以便统一理解。角色的命名通常是根据用户权限来配置的，同一级别的用户可以有相同的角色。

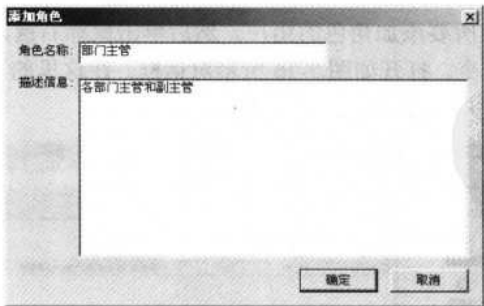


图 7-32 “添加角色”对话框

单击【确定】按钮，把新的角色添加进去，用同样的方法添加其他角色。添加角色后的权限管理界面如图 7-33 所示。

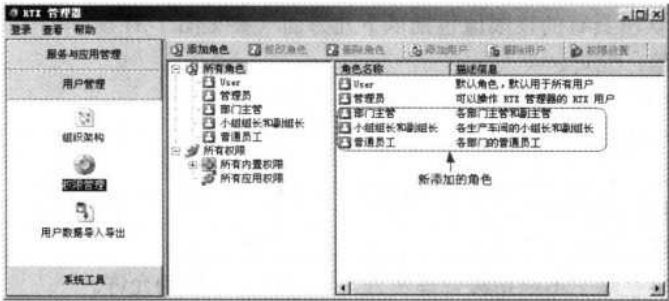


图 7-33 添加新角色后的“权限管理”界面

添加了角色后，可以为角色添加用户，方法是在如图 7-33 所示界面中选中某一角色，单击工具栏中的【添加用户】按钮，打开如图 7-34 所示对话框。在这里可以为这个角色添加用户。在“全部用户”文本框中可以直接输入要添加用户的 RTX 号码，当然也可以在下面的部门列表中选择相应的用户，然后单击【添加】按钮将用户添加到右边的“选中用户”列表中。不过，在此要注意的是这里所添加的用户一定要是在组织架构中添加了的。

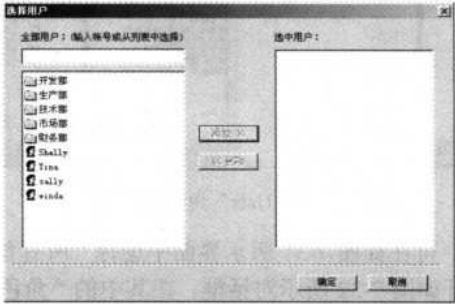


图 7-34 “选择用户”对话框

如要为某一角色批量添加某一组织架构下的多个用户，就得进入组织架构界面。然后在“全部用户”界面（如图 7-35 所示）下按住【Shift】按钮用鼠标连续多选，按住【Ctrl】按钮用鼠标间隔多选，选中所要添加角色的用户。然后单击鼠标右键，在弹出的快捷菜单中选择【为用户添加角色】命令，打开如图 7-36 所示对话框。在这里的“角色名称”列表中选择所要为用户添加的角色，单击【添加】按钮即可。



图 7-35 “组织架构”窗口“全部用户”标签界面

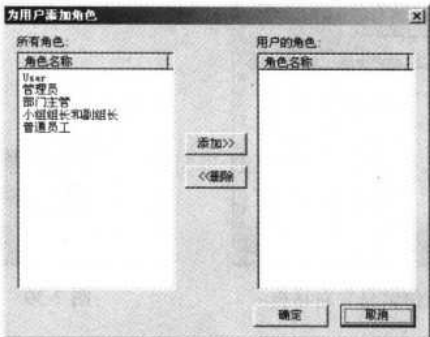


图 7-36 “为用户添加角色”对话框



顺便介绍一下，在 RTX 系统中默认创建了一个超级管理员账户，但如果想配置多个管理员账户（不是超级管理员），则可在系统内置“管理员”角色中添用户。方法是在如图 7-33 所示界面的“管理员”角色上单击鼠标右键，在弹出的快捷菜单中选择【添加用户】命令，打开如图 7-34 所示对话框。在其中添加要指派为管理员的用户账户。指派 RTX 用户为普通管理员后，用户可以用 RTX 账号和 RTX 密码以普通管理员的身份进行登录管理器，登录后的功能除了不能指派 RTX 成为普通管理员功能外，其他所有的功能都可使用。

如果是为单个用户配置角色，则可在如图 7-37 所示界面中通过单击【添加】按钮，打开如图 7-36 所示对话框进行添加。最后在如图 7-37 所示对话框中单击【应用】按钮即可生效。



图 7-37 “部门架构”窗口“用户角色”标签界面

如果要修改某角色，则需在如图 7-33 所示界面中选择某个要修改的角色（注意，一定是新添加的角色，不能修改内置的角色），再在工具栏中单击【修改角色】按钮，打开如图 7-38 所示对话框。在这里内可以对角色的名称和描述信息进行修改。

如果要删除某角色，则可以在如图 7-33 所示界面中选中某个角色，再在工具栏中单击【删除角色】按钮，打开如图 7-39 所示提示框。如果确认删除，则单击【确定】按钮即删除了该角色，但也只能删除新建的角色，不能删除 RTX 系统内置的两个角色。角色删除后，之前该角色下的用户对应的权限变为无效，但用户账户不会删除。

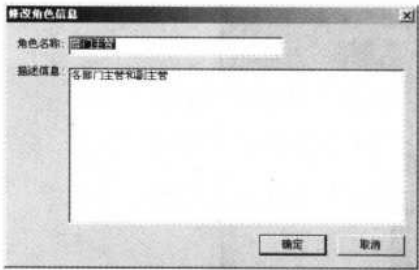


图 7-38 “修改角色信息”对话框

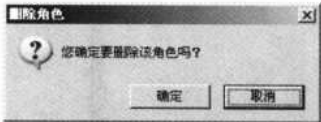


图 7-39 “删除角色”提示框

2. 权限说明

在如图 7-29 所示界面中间窗口中选择“所有权限”选项，即可看到所内置的权限选项，如图 7-40 所示。在权限列表中包括“修改姓名”、“发送短信”、“发起 30 人以上多人会话”、“发送大于 3MB 的文件”、“使用点对点方式传送文件”、“发送广播消息”等权限。下面是这些内置权限的简要说明。

- 发送短信：被赋予这个权限的用户可以通过 RTX 发送手机短信。
- 发起 30 人以上多人会话：被赋予这个权限的用户可以发起管理员指定人数以内的多人会话。
- 传送大于 3MB 的文件：被赋予这个权限的用户可以发送管理员指定大小的文件。
- 点对点方式传送文件：被赋予这个权限的用户可以使用点对点方式传送文件。
- 发送广播消息：被赋予这个权限的用户可以发送广播消息。
- 远程登录：被赋予这个权限的用户可以从其他上远程登录到本地 RTX 服务器。

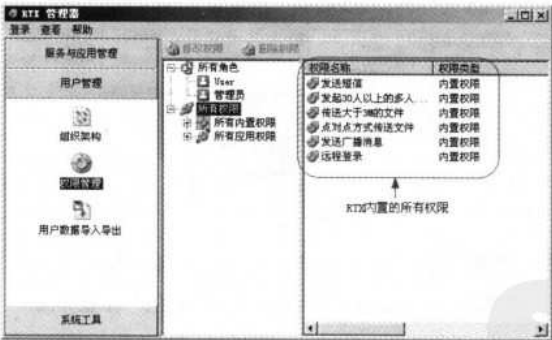


图 7-40 “所有内置权限”界面

用户所具有的角色权限以“允许优先”为准则，即用户属于不同角色的权限，如定义了不同的“允许”和“拒绝”值，则用户以“允许”优先。

权限分为三种：不允许（既不选择允许，也不选择拒绝）、允许和拒绝；优先级由低到高排序：不允许→允许→拒绝，拒绝权限最高。

以用户 shelly 为例，shelly 既是角色 A，又是角色 B。角色 A 设置允许“发送广播消息”，角色 B 设置拒绝“发送广播消息”的权限，则用户 shelly 最终的权限为不具有“发送广播消息”权限。

3. 权限的分配与回收

用户权限的分配与回收是通过角色来实现的。对用户分配权限的过程，实际上是为角色分配权限的过程。

要为角色配置权限，只需在如图 7-33 所示界面中选中某个角色，再在工具栏中单击【权限设置】按钮，打开如图 7-41 所示对话框。先在左侧窗口的权限列表中选择相应权限选项（可以在选择的同时按住【Shift】键连续多选，也可同时按住【Ctrl】键间隔多选）单击【添加】按钮添加到右边窗口中，然后再选择“允许”列中的复选框，即可完成权限的分配。当认为某项权限不再需要时，需先在右边窗口中选择要删除的权限项，然后单击【删除】按钮，即可完成对权限的回收。

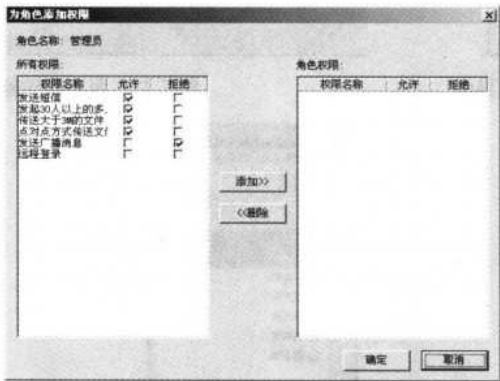


图 7-41 “为角色添加权限”对话框

权限选项选择完成后，单击【确定】按钮，即可完成一个角色权限的设置。用同样的方法设置其他角色，这样所有角色就全部分配了内置的用户权限。

7.5 客户端设置与使用

下载并安装 RTX 客户端程序后，就可启动客户端登录程序的初次登录。在通过客户端安装包完成安装之后，或者执行【开始】→【腾讯通】→【腾讯通 RTX】菜单操作，即可打开 RTX 客户端登录界面，如图 7-42 所示。

用户需要在“账号”和“密码”文本框中填写自己的 RTX 账号和密码。如果是第一次登录，则单击【登录】按钮，打开如图 7-43 所示服务器配置界面。在“服务器设置”栏的“地址”文本框中填写 RTX 服务器的计算机名或者 IP 地址，在“端口”栏中如果 RTX 服务器中的端口号没有改变，则不要更改。再单击【确定】按钮，回到如图 7-42 所示登录界面。再次单击【登录】按钮，即可开始登录了。登录成功后的界面如图 7-44 所示。其中显示的是相应用户所用的用户账户所在的 RTX 系统组织架构。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-42 RTX 客户端登录界面

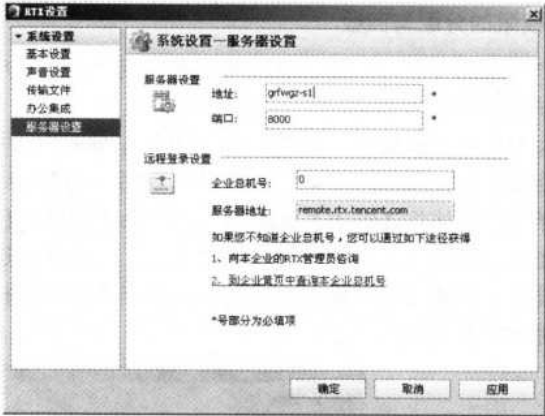


图 7-43 服务器设置界面



图 7-44 登录成功后的 RTX 客户端界面

7.5.1 个人设定

它与 QQ 一样，RTX 客户端也可以由用户设置自己的个人基本资料，如姓名、性别、年龄、联系方式等，还可以修改密码。不过本节不详细介绍，因为它与 QQ 的设置方法基本一样，相信大家已经熟悉了。本节仅将介绍四个主要的界面配置。

(1) 在如图 7-44 所示主界面中执行【文件】→【个人设置】菜单操作或者在 RTX 客户端状态栏 RTX 程序图标上单击鼠标右键，在弹出的快捷菜单中选择【个人设置】命令，都可以打开如图 7-45 所示对话框。在这里除了年龄、头像可以自己修改外，其他的都不可以。头像的修改可以在界面中单击右边的【更改】按钮，打开一个对话框进行修改即可。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-45 “个人设置”对话框中“基本资料”选项设置界面

(2) 在界面左边导航栏中单击选择“修改密码”选项，在右边窗口中即显示相应配置界面，如图 7-46 所示。对于初次登录 RTX 客户端的用户，管理员会建议用户将初始设定的密码修改为自己所熟知的密码，以便自己能正常、安全地使用该 RTX 客户端账号。在这里首先要输入该账户的原密码，然后再输入新密码（15 位以内）。只有当原密码正确，新密码符合要求的情况下才能进行密码修改。



图 7-46 “修改密码”选项设置界面

(3) 在界面左边导航栏中选择“热键设置”选项，在右边窗口中即显示相应配置界面，如图 7-47 所示。在这里可以根据自己的需求和习惯重新设置以上两个热键项。



图 7-47 “热键设置”选项设置界面

“热键设置”选项是对热键的使用进行设置。例如，默认的读取消息的热键是【Ctrl+Alt】组合键，即当收到消息的时候只要同时按下这两个键则可以读取消息，不需要用鼠标去双击读取。又如，【Ctrl+Alt+p】组合键时默认为截图热键，同时按下这三个键的时候就可以截取选定的区域。

对于熟悉电脑操作的用户，使用热键操作可以很大程度上提高工作效率，RTX 正是从这一角度出发，定义了方便的热键操作。如果在启动 RTX 的时候提示“热键冲突”，表示系统中已经有使用相同的热键操作，可以通过在如下的界面重新设置方便用户操作的热键。

(4) 在界面左边导航栏中选择“热键设置”选项，在右边窗口中即显示相应配置界面，如图 7-48 所示。在这里用户可以自己设定一个时间间隔，当电脑处于空闲状态超过这个时间时，让 RTX 自动转换离开或离线状态；通过设置固定回复留言，在 RTX 设置为离开状态时自动回复。



图 7-48 “回复设置”选项设置界面

在“留言栏”列表中可以先添加一些自动回复的留言，当要离开时，在这里选择相应的留言项，当状态转换到离开状态后，有人发送消息后即自动向对方回复所选择的留言。如果没有事先选择设置的留言，则会自动选择上一次的留言选择，或者排在最上面的那个留言。还可通过单击【添加】按钮添加新的留言，也可以通过【修改】按钮修改已有留言，通过【删除】按钮删除不需要的留言项。

7.5.2 系统设置

系统设置的方法与上面介绍的个人设置的方法基本一样，与 QQ 系统设置方法一样。它是对 RTX 客户端在所在计算机运行时的参数设置。

1. 基本设置

在如图 7-48 所示界面导航栏中，单击【系统设置】按钮，展开其下面的选项，选择“基本设置”选项，界面如图 7-49 所示。在这里可以设置客户端登录界面的风格，是否允许在接收到消息时弹出提示框，关闭程序时的状态，以及是否自动登录等选项。



图 7-49 “基本设置”选项设置界面

2. 声音设置

在如图 7-49 所示界面左边导航栏中选择“声音设置”选项，配置界面如图 7-50 所示。在这里可以对程序的场景声音进行设置。



图 7-50 “声音设置”选项设置界面

在这里不仅可以选择是否打开声音开关，还可为不同场景选择不同的提示声音（在“声音”下拉列表框中选择）。通过配置播放不同的声音文件（可以是自己录制的，或者其他来源的声音文件）来实现的。通过单击【播放】按钮可事先试听，不好的话，可以重新选择。

3. 传输文件设置

这项功能相对来说要重要些，因为通常我们习惯于把所有下载文件放在一个专门的目录，而不是直接放在 RTX 默认的文件夹中。

在如图 7-50 所示界面左边导航栏中选择“传输文件”选项，配置界面如图 7-51 所示。在这里可以设置一个默认接收传送文件的文件夹，还可设置该文件夹可使用空间的报警值。



图 7-51 “传输文件”选项设置界面

至于服务器设置已在如图 7-43 所示对话框中进行了介绍，在此不再赘述。

7.5.3 添加联系人

在 RTX 客户端组织架构面板中包括一个“联系人”项，它主要包括“常用联系人”、“自定义组”、“常用部门”栏目和“最近联系人”栏目，如图 7-52 所示。

1. 常用联系人

在这里列出当前 RTX 客户端用户自己所设置的常用办公联系人。用于快速地查找到某常用联系人，并对其发起操作。也可以通过单击鼠标右键，在弹出的快捷菜单中选择【添加联系人】命令，打开如图 7-53 所示对话框添加常用联系人（默认显示的只是已添加或者正在线的用户）。在“查找”文本框中直接输入在组织架构中已添加了的用户名，然后单击【查找】按钮即可在左边的列表中显示，然后选择该用户，再单击【添加】按钮即可把该用户添加到自己的常用联系人列表中。



图 7-52 RTX 客户端界面“联系人”栏目

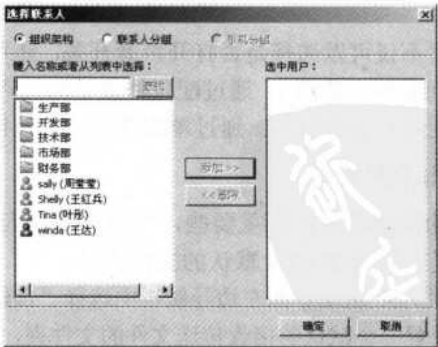


图 7-53 “选择联系人”对话框

2. 自定义组

在如图 7-52 所示界面中选择“自定义组”选项，单击鼠标右键，在弹出的快捷菜单中选

择【添加自定义组】命令，打开如图 7-54 所示对话框。在这里提供了用户因需要而自行定义讨论组的功能，与 QQ 中的用户组功能一样。

在“自定义组名称”文本框中输入自定义组的名称，然后单击【添加】按钮，打开的对话框参见图 7-53 所示。在其中选择自定义组的成员，依次在两个对话框中单击【确定】按钮就完成了自定义组的添加，如图 7-55 所示。



图 7-54 “自定义组设置”对话框

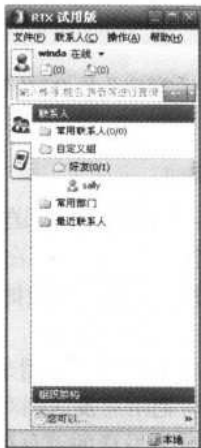


图 7-55 添加了自定义组成员后的“自定义组”界面

3. 常用部门

在如图 7-55 所示界面中的“常用部门”栏中列出的是当前 RTX 客户端用户自己所添加的常用部门。用于快速地查找到某部门，并对其发起操作。也可以通过单击鼠标右键，在弹出的快捷菜单中选择【添加常用部门】命令，打开如图 7-56 所示对话框。在对话框左侧的部门列表中选择常用部门（同样，可通过同时按住【Shift】键连续多选，或者按住【Ctrl】键间隔多选），然后单击【添加】按钮，即把所有已选为常用部门中的用户添加进去。这样也就把所有已选为常用部门的部门用户添加到“常用部门”栏下，如图 7-57 所示。

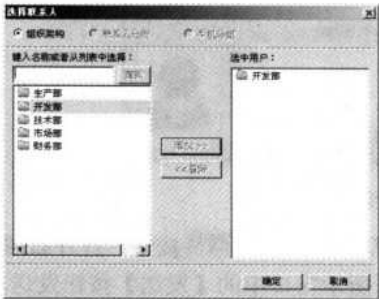


图 7-56 “选择联系人”对话框



图 7-57 添加“常用部门”后的“联系人”界面

4. 最近联系人

在如图 7-57 所示的“最近联系人”栏，是用来列出当前 RTX 客户端用户最近沟通的 20 个会话名单。可以单击鼠标右键，在弹出的快捷菜单中选择【清空最近联系人】命令，清空其中所列的所有最近联系人。

7.5.4 多功能会话

“多功能会话窗口”是 RTX 客户端一种基本的即时沟通工具。它与 QQ 的使用方法基本一样。

1. 发送消息

在 RTX 中，可以向对方发送消息的地方很多，在“联系人”栏中所有子栏中存在的用户都可以发送，而且可以在对方不在线的情况下给对方留言。方法是在要把信息发送给对方账户上单击鼠标右键，在弹出的快捷菜单中选择【发送即时消息】命令，打开如图 7-58 所示窗口。

在窗口的下半部分是自己用来输入要发送的消息的窗口，输入完所要发送的消息后单击【发送】按钮即可把消息发送到对方，窗口与如图 7-45 所示窗口一样；而上半部分窗口则是自己所有已收到或者发送的消息列表显示。在窗口的右边有两个头像显示，上边那个是对方的头像，而下边那个则是自己的头像。



当然，与 QQ 一样，RTX 不仅能发送文字消息，还可以发送图片、表情动画。如果要发送图片文件，则在如图 7-58 所示窗口中部单击 图片按钮，在打开的窗口中选择。如果是直接截取的图片，则可直接在下半部分文本窗口中粘贴，然后单击【发送】按钮发送。



图 7-58 RTX 会话窗口示例

要发送表情符，则可单击如图 7-48 所示窗口中部的 表情按钮，打开如图 7-59 所示窗口，在其中选择即可，然后同样单击如图 7-58 所示窗口中的【发送】按钮发送。

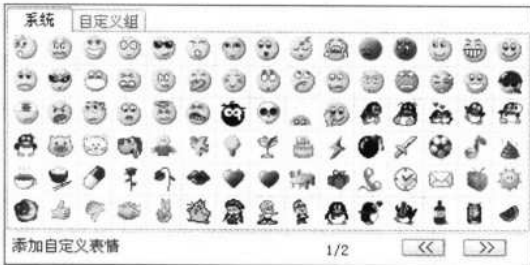


图 7-59 表情图窗口

同样，也可以像 QQ 那样，把自己发送的消息设置成有特色的字体、字号、颜色，以便与其他用户区别，特别是多人聊天，这个功能还比较实用。设置发送消息的文本字体、字号、颜色的方法是在如图 7-58 所示窗口中部单击“**字体**”按钮，打开如图 7-60 所示对话框，在这里就可以设置了。但要注意的是，这里的设置对所发送的文本都同时适用，不能局部改变字体、字号和颜色，只能是统一的。

2. 多人会议

如果想要多人聊天或者召开多人网上会议，则可在如图 7-58 所示会话窗口中单击工具栏中的  按钮，打开如图 7-61 所示对话框。

在其中把各部门中要参加多人会议的人全部选择（除了已在会话的人外，同样可通过同时按住【Shift】键连续多选，或者按住【Ctrl】键间隔多选），然后单击【添加】按钮一次性加入。当然也可以一个个单独添加，但这样效率低。最后单击【确定】按钮，即可在如图 7-58 所示窗口中见到一个提示消息，并且在窗口右上角会显示参加会议的人员列表。

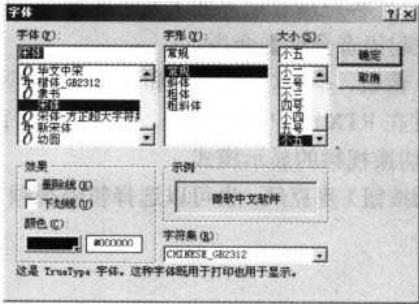


图 7-60 “字体”对话框

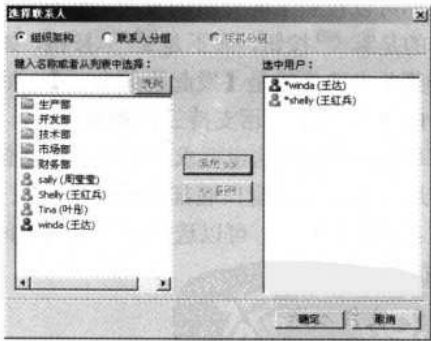


图 7-61 “选择联系人”对话框


多人会议的其他会话方法与两人聊天的相应操作方法完全一样，在此不再赘述。但这里发送的消息、图片、表情会在参会人员的话窗口中显示。



此时如果仅想与参加会议的某个人私聊，则可在如图 7-58 所示会话窗口的右上角参会人员列表中选择相应的人员，单击鼠标右键，在弹出的快捷菜单中选择【发送即时消息】命令，打开一个新的会话窗口进行私聊。





管理员可以通过角色权限设置用户是否有发起 30 人以上会话的权限，没有权限修改设置的人，只能最多添加 30 人进行会话，如果需要添加超过 30 人，则不能发起会话。有权限修改设置的用户，添加的人数没有限制。

3. 六人语音会议



新的即时通信窗口中，还实现了很多多媒体方面的功能。比如，多个人进行对话的时候，通过单击如图 7-58 所示会话窗口工具栏中的  语音按钮，可以轻松地实现多人音频的沟通，现在 RTX 支持六人同时语音会议。




要实现六人语音会议的方法有两种，一种是在如图 7-58 所示会话窗口先添加参加会议的人，然后主持人再单击会话窗口工具栏中的  语音按钮，在所有用户的语音设备和语音设置配置好后即可开始语音会议。在主持人单击  语音按钮后，会在所有其他用户上弹出提示信息，询问是否接受语音会议。当然对方必须安装好声卡和麦克风驱动程序。



发起语音会议的另一种方法是在 RTX 客户端登录界面中，通过按住【Shift】键（连续多选），或者按住【Ctrl】键（非连续多选）选择参与语音会议的人（目前最多为六人），然后单击鼠标右键，在弹出的快捷菜单中选择“发起语音会议”命令，同样会打开语音会议会话窗口。

在多人语音会话中，语音会话的发起者为这次会话的主持人。主持人可以删除或添加会话的参与者，也可以结束会话。添加的方法也是单击会话窗口工具栏中的  邀请按钮，在打开的对话框选择要邀请的用户；删除的方法是在语音会话窗口右侧用户列表中，选择要删除的用户，然后单击旁边的  按钮，在弹出的确认对话框中单击【是】按钮即可。


4. 高清晰视频

你可以按照上面介绍的发起语音会话的方式发起视频会话，不同的只是此处工具栏中单击的是  视频按钮，而不是  语音按钮，如果是在 RTX 客户端登录界面上发起的会话，则在快捷菜单中选择的是【发起视频会话】，而不是【发起语音会议】命令。

RTX 的视频会话支持三种视频模式，320×240 像素、640×480 像素和全屏幕，更支持全屏幕显示。当然这也要求双方有视频摄像设备，并在 RTX 客户端配置好。在视频会话窗口中，通过单击会话窗口底部的    三个按钮来切换视频的显示模式。

在视频过程中，可以选择开启或者关闭（单击  按钮）麦克风，也可以选择暂停视频（单击  按钮）。

5. 文件发送

除了即时信息与 QQ 一样，RTX 用户之间也可以进行文件的直接传送。通过单击如图 7-58 所示会话窗口工具栏中的  发送文件按钮，即可使用该功能。首先打开的是一个文件浏览窗口，在其中选择要发送的文件。选择好后即把所要发送的文件贴在会话窗口的下半部分窗口中，如图 7-62 所示。单击【发送】按钮，即可把文件发送给对方。在接收者收到新文件来到的信息提示后，双击该文件，打开一个如图 7-63 所示对话框，用户可以选择直接打开或者保存至某目录下。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 7-62 发送文件会话窗口示例

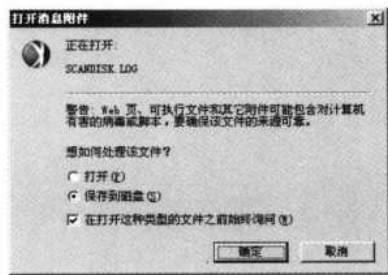


图 7-63 “打开消息附件”对话框

至于 RTX 客户端的其他功能在此就不一一介绍了，如各种各样的消息查看可以在客户端登录主界面中选择要查看的用户，单击鼠标右键，在弹出的快捷菜单中选择【查看消息记录】命令，在打开的如图 7-64 所示窗口查看即可，包括“会话消息”“多人会话消息”“接收的文件”、“广播消息”和“手机消息”等。



图 7-64 “消息管理器”窗口

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



第 8 章 企业流媒体服务器系统

随着互联网宽带的接入和 DDNS 的普及教育，现在单位甚至个人在互联网上（也可以在企业局域网内部）架设专业媒体服务器已变得非常容易。因为以前媒体服务器所要求的高带宽，现在像 10Mbps 的光纤接入已基本没有问题了，DDNS 又解决了以往域名解析的问题。在一些媒体、ICP（Internet 内容提供商）或者网吧，甚至一般的企业网络中，经常需要配置支持各种语音、视频的媒体播放服务器，为客户实现在线点播，也称之为 VOD（按需视频点播）。

通过媒体服务器的播放称之为“流式播放”，在其中播放的媒体又称之为“流媒体”。它是目前互联网媒体应用的主要媒体类型。流媒体文件不仅在格式上与我们平常在本地播放的媒体格式有些区别，而且在播放方式上也存在本质区别，那就是播放的媒体文件不用下载到客户端，不用占用客户端磁盘空间。而且客户端也可以进行各种本地播放一样的操作，如关闭、快进、快退、选择播放列表等。

目前常见的流媒体服务器配置方案有多种，如 RealNetwork 公司的 Real Server、Apple 公司的 Quick Time Streaming Server（QTSS）等。本章要介绍的是集成在微软公司 Windows Server 2003 R2 系统中的 Windows Media Services 9.0 系统。该版本所支持的媒体格式非常多，完全可以满足绝大多数用户的配置和应用需求。

本章重点

- Windows Media Services 9.0 版本的主要改进
- Windows Media Services 9.0 可支持的流媒体格式
- Windows Media Services 9.0 服务器的配置
- Windows Media Services 9.0 插件属性配置
- Windows Media Services 9.0 服务器系统的部署
- 发布点的创建与属性配置
- 流媒体内容的制作
- 流媒体广告内容的封装
- Windows Media 编码器的使用

8.1 流媒体基础

作为新一代互联网应用的标志，流媒体技术在近几年得到了飞速的发展。而流媒体服务器又是流媒体应用的核心系统，是运营商向用户提供视频服务的关键平台。其主要功能是对媒体内容进行采集、缓存、调度和传输播放，流媒体应用系统的主要性能体现均取决于媒体服务器的性能和服务质量。

流式播放是一种以数据包形式传输数字媒体的方法，这种方法在接收的同时呈现内容，从而可以连续地播放数据，而不必等待下载整个文件。这与传统的媒体播放方式完全不同。流媒体播放系统有多种，本章仅介绍基于微软 Windows Server 2003 R2 系统中自带的 Windows Media Services 9 系列播放系统的组建。

8.1.1 下载内容与流式播放

可使用流式播放或下载方法通过网络将数字媒体文件传递到客户端。

1) 下载

为了通过使用下载方法将内容传递给用户，通常需要先内容保存到 Web 服务器，并通过在网页上添加指向该内容的链接来向用户提供指向内容的链接。用户单击链接，便可将文件下载到其本地硬盘上，然后再使用播放机播放内容。

下载这种方式，需要用户先将既耗费时间又耗费磁盘空间的整个文件复制到其计算机中，然后才能播放。另外，因为整个文件必须在下载之后才能播放，所以，下载不能用于实况流。

同时，下载方式也不能高效地使用可用带宽。当客户端开始下载数字媒体文件时，所有可用网络带宽用于尽可能快地传输数据。因此，其他网络功能可能会减慢或被中断。

2) 流式播放

要通过使用流式播放方法将内容传递给用户，可以将内容保存到 Windows Media 或其他流媒体服务器上，然后再将该内容分配给发布点。不仅可以通过创建公告文件，或通过向用户提供发布点的 URL 来向用户提供对该内容的访问，还可以将公告文件或 URL 嵌入到网页中或将其以电子邮件形式发送。当用户单击链接或公告文件时，播放机就会打开并连接到相应的流。

流式播放以客户端正确播放所必需的速度通过网络进行数据传输，所以它可以比下载更高效地使用带宽。这有助于防止网络变得过载，并有助于维持系统的可靠性。因为播放机必须首先缓冲数据以防在流中存在延迟或间歇，所以在播放机接收流的时间和它开始播放流的时间之间通常有一个延迟。同时，因为对数据进行流式播放和呈现是同时发生的，所以流式播放还允许传递实况内容。

要想流畅地传输内容，内容的比特率必须低于网络带宽。如果内容的比特率高于可用带宽，则播放机将试图减弱流，以便它可以通过使用一个名为流缩减的过程来正确地呈现流。因此，播放机可以只呈现带有音频的视频流的关键帧，以便视频不再运转，并创建一个类似于幻灯片演示的观看体验。如果比特率要求大大超过可用带宽，则视频播放可能会完全停止，

而将只播放音频部分。

如果传输的是多比特率（MBR）内容，则客户端的可用带宽不足所带来的影响可以降到最小。MBR 内容允许播放机请求从服务器传输比特率较低的流，这样就无须减弱流。

3) 快速流式播放

Windows Media Services 9 系列包括的“快速流式播放”提供多项结合了流式播放和下载的功能。服务器可使用快速启动和高级快速启动功能来确保客户端在传输开始之后尽可能快地开始播放内容。快速启动功能允许播放机在开始播放内容之前，以网络所允许的最快速度从服务器下载和缓存一小部分内容。当填满播放机上的缓冲区之后，服务器将减慢流的传输，直到与播放机的呈现速度一致。

使用高级快速启动功能时，客户端在播放机缓冲区填满之前即可开始播放内容，从而使服务器能够更好地实现快速流式播放。只要播放机接收的数据达到最低的数据量要求，它就可以开始播放内容。播放机缓冲区继续以高于内容编码比特率的加速速率填充。缓冲区填满后，高级快速启动功能停止，这时播放器开始以编码比特率接收数据。

当服务器使用快速缓存功能时，服务器就会以尽可能高的比特率将所有内容传输到播放机，以使网络阻塞或中断所带来的影响降到最小。与普通的流式播放一样，当缓存了所需数量的数据之后，播放机立即开始呈现内容。数据的其余部分则存储在客户端的临时缓冲区中。

如果要传输可变比特率（VBR）内容，那么传输该流所需的带宽量会因所传输内容的复杂程度而变化。快速流式播放可通过向播放机发送额外数据以补充内容缓冲区来利用低带宽周期，并使得 VBR 内容从服务器传输时流畅地播放。



注意

快速流式播放只适用于在以下操作系统版本中运行的 Windows Media Services 9 系列：Windows Server 2003 Enterprise Edition 和 Windows Server 2003 Datacenter Edition。如果运行的是 Windows Server 2003 Standard Edition，那么此功能将得不到支持。

8.1.2 流式媒体系统概述

基于 Windows Media 技术的流式播放媒体系统通常由运行编码器（如 Microsoft Windows Media 编码器）的计算机、运行 Windows Media Services 的服务器和播放机组成。编码器允许将实况内容和预先录制的音频、视频和计算机屏幕图像转换为 Windows Media 格式。运行 Windows Media Services 的服务器名为 Windows Media 服务器，它允许通过网络分发内容。用户通过使用播放机（如 Windows Media Player）接收分发的内容。整个系统结构和播放流程如图 8-1 所示。

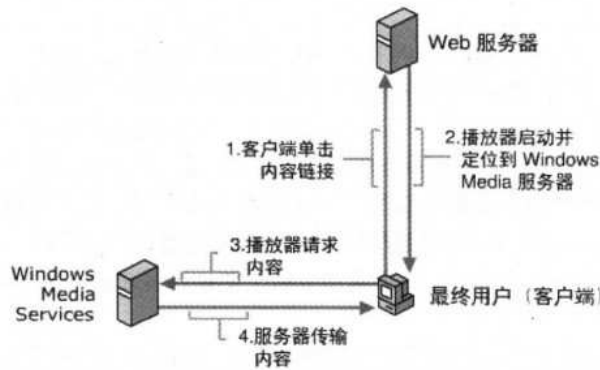


图 8-1 Windows Media Services 流式媒体系统结构和播放流程

通常情况下，用户通过在网页上单击链接来请求内容。Web 服务器将请求重新定向到 Windows Media 服务器，并在用户的计算机上打开播放机。此时，Web 服务器在流式播放媒体过程中不再充当角色，Windows Media 服务器与播放机建立直接连接，并开始直接向用户传输内容。Windows Media 服务器获取流媒体源的途径如图 8-2 所示。

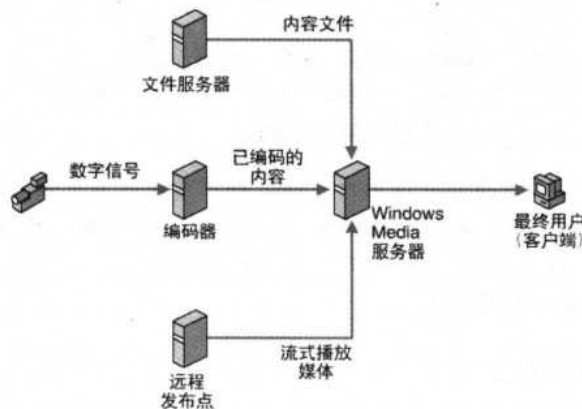


图 8-2 Windows Media 服务器获取流媒体源的途径

Windows Media 服务器可从多种不同的源接收内容。预先录制的内容可以存储在本地服务器上，也可以从联网的文件服务器上提取。实况事件则可以使用数字录制设备记录下来，经编码器处理后发送到 Windows Media 服务器进行广播。Windows Media Services 还可以重新广播从远程 Windows Media 服务器上的发布点传输过来的内容。

8.1.3 了解 Windows Media 9 系列

Windows Media 9 系列是指由 Microsoft 公司开发的数字媒体软件系列。其中所有产品的设计目的都是为了协同工作，以提供最佳的数字媒体体验。

Windows Media Services 是一种通过 Internet 或 Intranet 向客户端传输音频和视频内容的平台。这些客户端可以是使用播放机（如 Windows Media Player）播放内容的其他计算机或

设备，也可以是用于代理、缓存或重新分发内容的运行 Windows Media Services 的其他计算机（称为 Windows Media 服务器）。客户端也可以是使用 Windows Media 软件开发工具包（SDK）开发出来的自定义应用程序。

Windows Media 服务器流式传输给客户端的内容可以是实况流，也可以是预先存在的内容，例如，数字媒体文件。如果计划传输实况内容，服务器将连接到能够以服务器支持的格式广播实况流的编码软件（如 Windows Media 编码器）。也可以传输使用 Windows Media 编码器、Microsoft Producer for PowerPoint 2002、Windows Movie Maker、Windows Media Player 或许多其他第三方编码程序编码的预先存在的内容。

Windows Media Services 9 是经过重新设计的，使服务器更加灵活、统一了核心组件并简化了管理过程。以下是这一版本所作更改的简要概述。

1) 服务四合为一

Windows Media Services 服务取代了 Windows Media Services 4.0 和 4.1 版本所包含的四个单独的服务：Windows Media Monitor Service、Windows Media Program Service、Windows Media Station Service 和 Windows Media Unicast Service。

2) 插件的扩展使用

如果使用 Windows Media Services 4.x 版本，则可以使用自定义验证插件、授权插件或事件通知插件来扩展服务器，但不支持其他插件类型。此版本通过扩展的插件结构大大增加了用于自定义和配置服务器的方法数，已为大部分插件提供了界面，因此可以建立提高服务器性能的自定义插件。同时可以使用插件控制如下行为。

- 服务器如何从设备读取：使用数据源插件使服务器能够读取数据库、设备驱动器和各种网络位置。
- 如何在网络上发送数据：将数据写入器插件与控制协议插件一起使用以支持各种网络协议。
- 如何转化服务器端播放列表：使用播放列表分析程序插件以使服务器可支持各种不同的元文件格式。

3) 发布点的扩展使用

发布点扩展了 Windows Media Services 早期版本提供的基本功能，并且大大简化了以前由节目、流和广播站联合提供的功能。现在可以同时创建广播发布点和点播发布点，而且可以通过可控制不同服务器功能的属性界面来自定义这些发布点。

4) 灵活的服务器端播放列表

每个发布点（包括点播发布点）都可以传输播放列表的内容。播放列表中的每个项目都具有一组独立的属性，如重复、持续时间、类型等属性。可以指定这些属性来满足具体需要。甚至可以在广播过程中修改播放列表，以使不必中断流即可响应此情况。

5) 灵活的事件结构

在 Windows Media Services 早期版本中，只能通过广播站和单播 Microsoft ActiveX 对象来获得外部事件。在此版本中，外部可以同时通过 Windows 管理规范（WMI）事件和简单网络管理协议（SNMP）事件获得事件，而内部则可以通过服务器界面来获得事件。

6) 快速传输

在 Windows Media Services 早期版本中，内容以恒定的比特率传输到客户端。“快速传输”

476 网管员必读——网络应用（第2版）

允许传输、下载和缓冲联合使用以便提供最好的用户使用效果。以下功能提供了“Windows Media Services 快速传输”功能。

- 快速启动：使内容的开始部分以最大可得带宽迅速下载到 Windows Media Player，减少了充满播放机的缓冲要求所需的时间和用户开始接收流时必须等待的时间。
- 快速缓冲：使 Windows Media Services 可充分利用任何其他带宽将额外的数据发送到播放机的缓冲区，以便允许播放机可以更好地承受网络带宽波动。
- 快速恢复：通过使用转发纠错大大减少数据包损坏和中断事件，使服务器为那些在延迟时间较长的网络连接上（如无线网络和卫星网络）接收内容的用户提供不间断的查看效果。
- 快速重连：使服务器自动恢复在广播过程中由于网络问题而丧失的客户端连接，包括编码器、分发服务器和播放机。

7) 数据包重发逻辑性能提高

在 Windows Media Services 早期版本中，客户端数据包重发请求仅能实现最后 2 秒的内容。在此版本中，有了更好的纠错和流质量，可将 10 秒的数据存储在服务器缓冲区中。

8) 基于服务器的内容重包装

在 Windows Media Services 早期版本中，服务器仅能传输由流格式定义的数据包。在此版本中，服务器可以设置最适宜的数据包大小以适合在环境中传输，并且服务器能根据此属性设置重新分配数据来传输数据包。这种优化仅当使用用户数据报协议（UDP）数据包和实时传输协议（RTSP）来传输内容时才适用。

9) 支持 IPv6 协议

此 Windows Media Services 版本支持 Internet 协议版本 6（IPv6）寻址。

10) 支持 IGMPv3

Internet 组管理协议（IGMP）版本 3 为 Windows Media Services 提供了帮助防止多个广播服务器使用同一多播 IP 地址出现的问题的能力。此功能要求连接到多播的客户端使用 Windows Media Player 9 系列。

8.1.4 与流式媒体播放有关的术语

本节所介绍的一些术语对于理解流媒体及播放原理、运用非常重要。

1) 元素

元素是一种扩展标记语言（XML）术语，指的是播放列表的“构建模块”。当用在播放列表文件中时，元素可以定义时间线、创建内容组，以及定义播放列表各部分之间彼此交互的方式。

2) 编码器

编码器是指一台计算机，它使用软件（如 Windows Media 编码器）将压缩/解压缩（codec）算法和流格式应用到采用模拟或数字音频和视频格式的内容上，然后将内容重新生成成为数字文件或流的过程称之为编码。对内容进行编码后，即可通过 Windows Media Services 进行分发。大多数情况下，用于内容编码的软件安装在不同于 Windows Media Services 的一台单独的计算机上。

3) 播放列表文件

Windows Media Services 可使用播放列表文件通过发布点向用户传输内容序列（例如，数字媒体文件、编码器 URL 和其他内容服务器位置）。播放列表文件既可以位于服务器端，也可以位于客户端。服务器端播放列表文件允许在客户端接收内容的同时管理服务器上的播放列表。客户端播放列表将传递给播放机，由播放机管理所有的内容项目。在客户端播放列表中，服务器不能修改其内容引用。

4) 公告文件

公告文件是一种 Windows Media 元文件，其扩展名是.asx，用于将客户端重定向到 Windows Media 服务器上的内容。公告文件可以从网站分发到客户端、作为电子邮件附件发送，或者在网络驱动器上共享。默认情况下，公告文件与 Windows Media Player 相关联。公告文件使用可扩展标记语言（XML）语法，可包含额外信息供播放机显示，例如，文件属性和字幕信息。公告文件也可包含针对播放机的其他指示，例如，指示播放机打开网页或向服务器发送日志记录数据。

在 Windows Media Services 管理单元中，可使用单播公告向导创建公告文件。如果使用多播传输，则可在使用多播公告向导创建多播信息文件时创建公告文件。具体将在本章后面详细介绍。

5) 带宽

带宽是反映网络数据传输能力的一种度量方法。带宽通常以系统每秒传输的比特数来表示：比特/秒（b/s）或千比特/秒（Kb/s）。向客户端传输内容时，Windows Media Services 会利用可用网络带宽。服务器中的每个流都有一个带宽要求，连接到服务器的客户端已根据其网络连接方法定义了可用带宽。因此，规划流媒体系统时，必须包括对不同带宽的支持。多播流式播放是一种在内部网上节约带宽的常用方法，因为它只在网络上发送一个流。

6) 发布点

发布点是向用户分发内容的途径。内容可通过创建将客户端重定向到发布点的公告文件来发布，也可通过分发指向发布点的 URL 来发布。

7) 拉传递

拉传递是从流来源（例如，Windows Media 编码器或另一个 Windows Media 服务器）向发出请求的 Windows Media 服务器传输内容的一种方法。拉传递用于指明流的传输是由请求服务器发起和管理的。

8) 推传递

推传递是从 Windows Media 编码器向 Windows Media 服务器传输内容的一种方法。推传递用于指明流的传输是由编码器启动和管理的。

9) 广播

广播是一种同时向大量观众传输数据的方法。在 Windows Media Services 中，广播是通过使用广播发布点来实现的。接收广播的客户端不能控制内容的开始和播放频率，也不能让流快进或倒回，该流由服务器控制。在客户端可从广播发布点接收内容之前，必须启动发布点。

478 网管员必读——网络应用（第2版）

10) 内容

内容是一个通用术语，指的是数字媒体文件或流中包含的音频、视频、图像、文本或其他信息。可将内容作为发布点的源，并通过 Windows Media Services 在网络上流式传输内容。

11) 提示

提示是一种将广播播放列表中的内容预加载到服务器内存中的方法。这样可以在将内容传输给客户端时缩短延迟时间。默认情况下，当先前的内容完成 90% 时，将提示播放列表序列中的下一项。如果要在广播期间跳过某个播放列表条目，那么对条目进行提示可以提供一种较好的播放体验。提示播放列表中的元素这一操作可在广播内容的发布点的“源”标签上完成。

12) 分发

分发是从一台计算机向另一台计算机传输内容的过程。使用 Windows Media Services 时可采用下列分发类型。

- 服务器到服务器的分发：当服务器上的发布点充当另一个 Windows Media 服务器上的发布点的内容源时进行的是这种分发，而后一发布点再将内容传输给发出请求的播放机。
- 推分发：当编码器主动发起广播时进行的是这种分发，此后编码器通过 Windows Media 服务器上的发布点将内容传输给发出请求的播放机。
- 拉分发：当服务器主动与编码器连接以接收内容流时进行的是这种分发，此后服务器将内容分发给发出请求的播放机。

13) 无序播放

无序播放是一种播放方法。它将目录或播放列表文件引用的内容随机化，之后再从发布点进行流式播放。无序播放内容时，将以随机顺序对播放列表或目录中的每一项进行播放。无序播放可与循环播放一起使用，以提供连续随机播放功能。必须为服务器启用 WMS 播放列表转换插件时，才能对播放列表或目录中的内容进行无序播放。可通过 WMS 播放列表转换插件的属性页关闭和打开无序播放。

14) 流式播放

流式播放是一种以数据包形式传输数字媒体的方法。这种方法在接收的同时呈现内容，从而可以连续地播放数据，而不必等待下载完整文件时再播放。

15) 单播

单播是一种通过网络传输数据包的方法。该方法要求在客户端和传输数据的服务间进行点对点通信。单播也称为定向通信，这是因为数据被定向到网络上的特定客户端。

8.1.5 配置 Windows Media 9 流媒体服务器系统的基本思路

配置 Windows Media 9 流媒体服务器系统的基本思路相对来说还是比较简单的，具体步骤如下。

（1）安装 Windows Media 9 流媒体服务器系统所需的组件。

这一步很简单，只需通过“控制面板”中的“添加或删除程序”工具即可完成。具体步骤参见本章后面的 8.2 节。

（2）流媒体服务器配置。

可能还希望实施通过 Windows Media Services 使用的一些更高级的功能。例如，你可以修改设置以限制客户端连接数、设置安全措施以保护内容、记录有关客户端活动的的数据，以及设置分发服务器。

在选择要使用的发布点类型时，应当考虑如何传递内容。以单播流方式传递内容时既可以采用点播发布点，也可以采用广播发布点；以多播流方式传递内容时只能采用广播发布点。利用单播流，客户端连接到 Windows Media 服务器以访问内容。利用多播流，服务器向网络上的单个多播 IP 地址传输内容，所有客户端都访问该 IP 地址（而不是连接到服务器）以接收流。因为单播流能够满足多个客户端请求，所以这将降低网络上所需的带宽量。

具体的流媒体服务器配置方法参见本章后面的 8.3 节。

（3）部署 Windows Media 9 流媒体服务器系统。

在正式配置 Windows Media 9 流媒体服务器之前，先要就整个流媒体服务器系统进行整体部署，主要考虑媒体内容的发布方式、网络带宽、媒体容量、服务器安全性、服务器容错性能、服务器均衡和可扩展性能等。

具体考虑参见本章后面的 8.4 节。

（4）添加和配置发布点。

Windows Media 9 流媒体服务器使用发布点将客户端对内容的请求转换为安置该内容的服务器的物理路径。可以向 Windows Media 9 服务器添加两种类型的发布点：广播发布点和点播发布点。如果要传输编码器的实况内容，最好选择广播发布点。如果打算传输文件且希望允许用户控制内容的播放（如暂停、倒回或快进），则最好选择点播发布点。

在已经添加了发布点和标识了要从中传输的内容之后，需要通知用户该内容可用。可通过为该内容创建公告来方便地完成通知操作。

发布点的添加与配置步骤参见本章后面的 8.5 节。

（5）内容制作和管理。

有时可能还需要自己录制一些影视媒体，即使有现成的媒体，我们在发布的时候也可能需要制作专门用途的媒体列表。还可能需要在媒体播放过程中插入一些广告内容。

具体内容制作和管理方法参见本章后面的 8.6 节。

本章最后一节（8.7 节）是可选阅读小节，介绍的是 Windows Media 编码器的基本使用方法。

8.2 流媒体服务器安装

随着 Internet 和 Intranet 应用日益丰富，视频点播也逐渐应用于宽带网和局域网。人们已不再满足于浏览文字和图片，越来越多的人更喜欢在网上看电影、听音乐。而视频点播和音频点播功能的实现，则必须依靠流媒体服务技术。

就目前来看，最流行的流媒体点播服务器只有两种，即 Windows Media 服务和 Real Server。本章要介绍的仅是如何在 Windows Server2003 平台利用系统自身的 Windows Media 服务组件搭建视频点播服务器。通常格式的文件必须完全下载到本地硬盘后，才能够正常打开和运行。而由于多媒体文件通常都比较大，所以完全下载到本地往往需要较长时间等待。

Windows Media 服务的流媒体格式文件只需先下载一部分在本地，然后可以一边下载一边播放。Windows Media 服务支持 ASF 和 WMV 格式的视频文件，以及 WMA 和 MP3 格式的音频文件。

8.2.1 Windows Media 服务的安装

Windows Media 服务虽然是 Windows Server 2003 系统的组件之一，但是在默认情况下并不会自动安装，而是需要用户来手动添加。在 Windows Server 2003 操作系统中，安装 Windows Media 服务组件的方法有两种：一种方法是直接利用“控制面板”中的“添加或删除程序”工具进行组件的安装；另一种方法是利用通用的“配置你的服务器向导”进行。在此分别予以介绍。

1. “添加或删除程序”法

这一方法中，Windows Server 2003 系统中的 Windows Media 服务组件安装非常简单，因为它所需的组件都在“Windows Media Services”选项中。安装方法与其他组件的安装方法是一样的，具体步骤如下。

(1) 执行【开始】→【控制面板】→【添加或删除程序】菜单中操作，打开如图 8-3 所示界面。

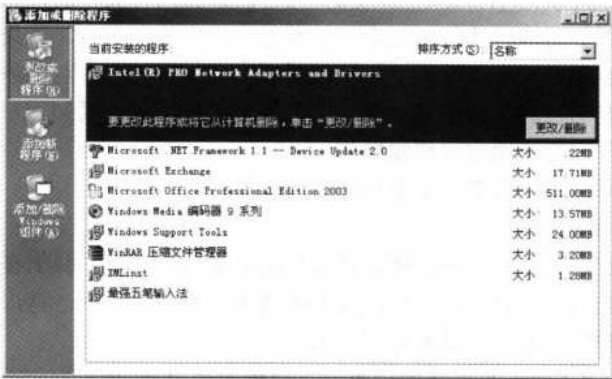


图 8-3 “添加或删除程序”界面

(2) 在左边导航栏中单击【添加/删除 Windows 组件】按钮，打开如图 8-4 所示的对话框。选择“Windows Media Services”复选项，单击【详细信息】按钮，打开如图 8-5 所示的对话框。

在其中确认至少选择了“Windows Media Services”和“Windows Media Services 管理单元”（用于流媒体服务器管理）两个复选项。如果要有多播和广告客户端的日志记录代理功能，则还可选择“多播和广告日志记录代理”复选项；如果还要通过 Web 远程管理这个流媒体服务器，则还需要选择“用于 Web 的 Windows Media Services 管理器”复选项，不过，此时需要安装了 IIS 组件。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-4 “Windows 组件向导”对话框



图 8-5 “Windows Media Services”对话框

(3) 单击【确定】按钮返回到如图 8-4 所示的对话框中。单击【下一步】按钮，系统会自动完成后面的组件安装，此时系统会提示 Windows Server 2003 系统源程序的路径，以便复制所需文件。完成后弹出“向导完成”对话框，即表明 Windows Media Services 服务组件已完善了，相应的流媒体服务器也就基本创建好了，直接单击【完成】按钮即可。

2. “配置你的服务器向导”法

这种方法是 Windows Server 2003 系统中所有服务器配置的通用方法，如域控制器、DNS 服务器、DHCP 服务器、WINS 服务器、文件服务器、流媒体服务器、邮件服务器等。整个操作流程比较简单，下面是具体的操作步骤。

(1) 执行【开始】→【管理工具】→【配置你的服务器】菜单操作，打开如图 8-6 所示对话框。

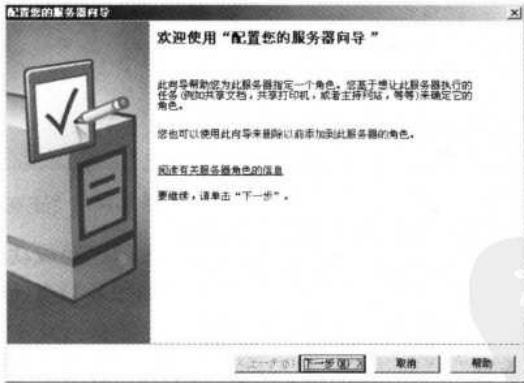


图 8-6 “欢迎使用‘配置你的服务器向导’”对话框

(2) 单击【下一步】按钮，打开如图 8-7 所示的对话框。在这里提示了要进行服务器安装必须做好的准备事项，确认全部做好后继续进行。

(3) 单击【下一步】按钮，打开如图 8-8 所示的对话框。在“服务器角色”列表中列出了所有可以安装的服务器。系统中大部分服务的安装和卸载都可以在该对话框中进行选择。选择列表中的“流式媒体服务器”选项。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

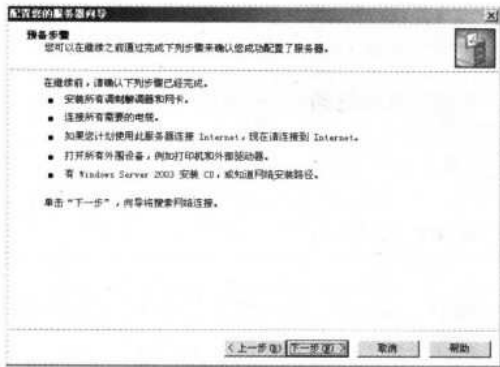


图 8-7 “预备步骤”对话框



图 8-8 “服务器角色”对话框

(4) 单击【下一步】按钮，将显示如图 8-9 所示的“选择总结”对话框，用来查看，并确认所选择的选项。

(5) 单击【下一步】按钮，打开如图 8-10 所示的“正在配置组件”对话框，并根据提示将 Windows Server 2003 安装光盘放入光驱。放入安装光盘后单击【确定】按钮，系统便开始从光盘中复制文件并安装 Windows Media 服务，并用进度条代表当前的安装进度。

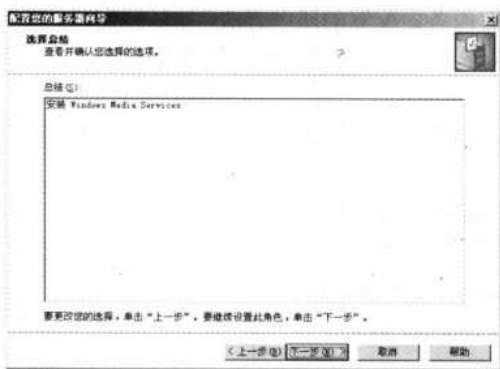


图 8-9 “选择总结”对话框

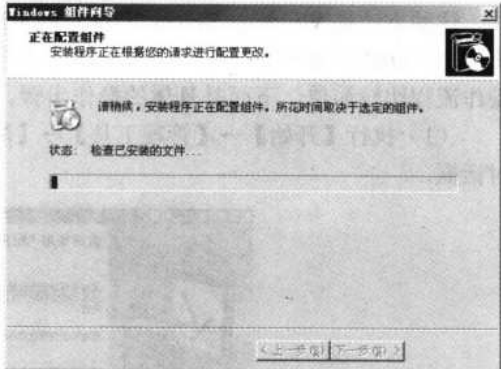


图 8-10 “正在配置组件”对话框

安装完成以后将显示一个“向导完成”对话框，这表示已经成功地将此服务器设置为流式媒体服务器。单击【完成】按钮关闭该向导，返回到如图 8-11 所示的“管理你的服务器”窗口，将显示流式媒体服务器已成功安装。

单击“流式媒体服务器”栏右边的“管理此流式媒体服务器”链接，或者执行【开始】→【管理工具】→【Windows Media Services】菜单操作，均可打开“流式媒体服务器控制台”界面，如图 8-12 所示。

在该界面中介绍了关于流媒体的一些基础知识，以作为入门者对它的了解。在“入门”选项卡中，单击左侧流媒体基础知识中的某个选项，即可在右侧显示出关于该选项的解释说明。在控制台左侧的控制台树上选择相应的流式媒体服务器（本示例为 XINHUA-S1），在右边详细信息窗口中再选择“入门”标签，不仅有基本流方案创建指引，还有更加详细的入门教程，如图 8-13 所示。单击下部的“启动 Windows Media Services 教程”链接前面的箭头，

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

可启动多媒体教程，如图 8-14 所示。下面的其他 3 个链接都有相应的多媒体教程。



图 8-11 “管理你的服务器”窗口



图 8-12 “流式媒体服务器控制台”界面



图 8-13 流式媒体服务器窗口中的“入门”标签




图 8-14 Windows Media Services 的多媒体教程

8.2.2 Windows Media 编码器的安装

Web 服务可用来发布 HTML 文件，而视频点播服务是用来发布流媒体文件的。使用 Windows Media 编码器（其实也可以是其他类型的编码器，只要支持 Windows Media Services 即可，在此仅以 Windows Media 编码器为例进行介绍），可以将文件扩展名为.wma、.wmv、.asf、.avi、.wav、.mpg、.mp3 之类的媒体文件和.bmp、.jpg 之类的图片转换为 Windows Media 服务使用的流文件。.asf、.wma 和.wmv 文件扩展名代表标准的 Windows Media 文件格式。其中的.asf 文件扩展名通常用于使用 Windows Media Tools 4.0 创建的基于 Microsoft Media 的内容，而.wma 和.wmv 文件扩展名是作为 Windows Media 编码器的标准命名约定引入的，目的是使用户能够容易区别纯音频（.wma）文件和视频（.wmv）文件，这三种扩展名可以交换使用。

Windows Server 2003 中并没有自带 Windows Media 编码器，需要到 Microsoft 官方网站上下载 Windows Media 编码器的简体中文版，然后再执行安装过程。Windows Media 编码器可以在微软的官方网站下载，不过要对应选择 Windows Media 9 系列的编码器。

**注意**

编码器既可以安装在 Windows Media 服务器上，同时也可以安装在其他计算机上。也就是说，编码器只需安装在执行编码（转换文件格式）工作的计算机上。

这款软件的安装与其他 Windows 系统软件的安装没什么区别，在安装的首个界面中即显示了该编码器软件所包括的基本模块，如图 8-15 所示。安装完成后根据系统提示重新启动计算机。然后执行【开始】→【程序】→【Windows Media】→【Windows Media 编码器】菜单操作，打开如图 8-16 所示的“Windows Media 编码器”主界面（每次启动时会自动打开“新建会话”窗口）。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 8-15 Windows Media 编码器 9 系列安装对话框中的首界面

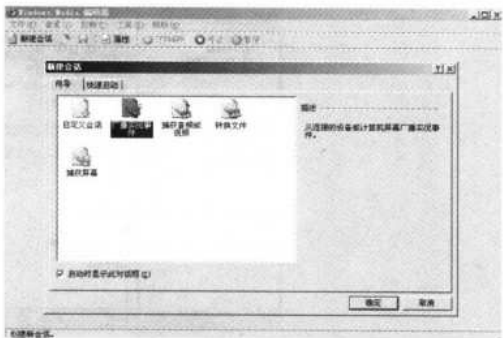


图 8-16 “Windows Media 编码器”主界面

8.3 Windows Media Services 服务器配置

Windows Media Services 流式媒体服务器安装好后，也需要进行一些基本的属性配置（主要是其安装的插件），以满足实际各方面的应用需求。流式媒体服务器属性的配置是通过它所包括的各个插件来进行的。配置方法只需在如图 8-13 所示窗口的右边窗口中选择“属性”标签，即可打开如图 8-17 所示插件属性配置窗口，在这里就可以配置所有插件的基本属性了。在如图 8-17 所示的“常规”选项中，没什么需要配置的，只是显示了服务器系统的版本。本节要介绍其他几个主要插件属性的配置知识。



图 8-17 流媒体服务器属性窗口“常规”选项配置界面

8.3.1 “授权”插件属性配置

在图 8-17 所示界面中选择“显示所有插件类别”复选项，在“类别”列表中选择“授权”选项，打开如图 8-18 所示配置界面。

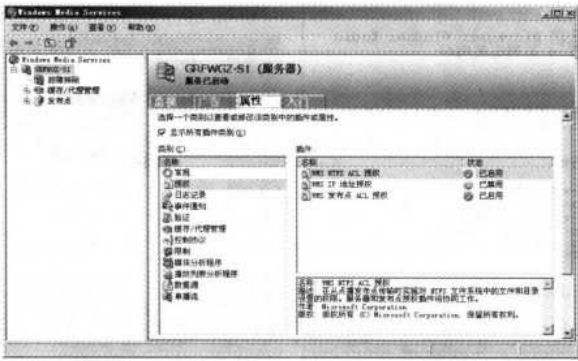


图 8-18 流媒体服务器属性窗口“授权”选项配置界面

要理解连接尝试被接受或拒绝的原因，很重要的一点是了解身份验证和授权之间的区别，身份验证是对尝试连接到服务器的客户端的凭据进行验证的过程。此过程包括从客户端向服务器发送凭据，以及使用身份验证方案识别用户。而授权是验证是否允许客户端连接到服务器的过程。授权在身份验证成功之后进行。在授权过程中，服务器按照为用户试图连接的资源设置的访问权限对用户进行检查。

可以启用授权插件来控制已通过身份验证的用户对内容的访问。如果启用了授权插件，那么还要启用身份验证插件以使用户能够访问发布点。然而，WMS IP 地址授权插件不需要身份验证插件即可对播放机进行身份验证。

可以在服务器和发布点级别启用授权插件。如果为服务器启用了授权插件而为服务器上的发布点启用了另一个授权插件，那么两个授权插件都将用于向用户授权，但服务器的插件将优先使用。如果为服务器或发布点启用了多个授权插件，那么将按照这些插件在服务器或发布点的“属性”标签上出现的顺序依次使用。如果任一插件拒绝用户访问，那么授权过程将终止，并且服务器将检查是否启用了其他身份验证插件对用户进行身份验证。

1. 使用 WMS NTFS ACL 授权插件

如果在 NTFS 文件系统中的文件和目录上设置了访问权限，那么可以启用 WMS NTFS ACL 授权插件来使这些权限生效。此插件将使 NTFS 文件系统中的文件和目录上设置的自定义访问控制列表（DACL）和系统访问控制列表（SACL）生效。DACL 是被允许或拒绝访问 Active Directory 对象的用户账户、组和计算机的列表。SACL 定义的是为用户、组或计算机审核的事件。当需要为内容设置不同的访问控制策略时，可使用此插件。

服务器和发布点授权插件将协同工作，WMS NTFS ACL 授权插件可以对特定的点播发布点或对整个服务器启用。一旦此插件启用，必须对从发布点或服务器播发的每一篇内容进行授权，以便由身份验证插件指定的用户账户访问。这就是说，如果你要从播放列表播放内容，那么用户账户必须得到访问播放列表中列出的所有项目的授权。如果用户账户无法通过播放列表中某一个项目的身份验证，那么将跳过该项目，并将播放列表中下一个身份验证成功的项目播放给客户端。

此插件使得在文件或目录上设置的访问控制策略生效，它不适用于下列情况。

1) 广播实况流

因为编码器中的流不位于 NTFS 驱动器上的文件或目录中，所以此插件无法用于实况流授权。

2) 代理流

在使用 Windows Media 服务器作为不缓存内容的代理服务器时，WMS NTFS ACL 授权插件没有明确的文件或目录集可以用来对照进行用户账户身份验证。在源服务器上启用 WMS NTFS ACL 授权插件将导致代理服务器向客户端转发授权请求并将信息传输回源服务器，然后由源服务器进行授权。如果要对访问代理服务器的客户端进行授权，请改用 WMS 发布点 ACL 授权插件。



注意 身份验证插件和授权插件协同工作，以便授予客户端访问流式媒体内容的权限。如果启用了 WMS NTFS ACL 授权插件或 WMS 发布点 ACL 授权插件，却没有启用身份验证插件，那么单播客户端将无法访问服务器。此插件依赖于从 NTFS 文件系统中搜集的信息，而该文件系统需要由 WMS 文件数据源插件访问。默认情况下，在安装 Windows Media Services 时，WMS 文件数据源插件是启用的。如果要使用此授权插件，请不要禁用 WMS 文件数据源插件。

2. 使用 WMS IP 地址授权插件

可以通过启用 WMS IP 地址授权插件基于特定的 Internet 协议（IP）地址，或 IP 地址组允许或拒绝对内容的访问。在只允许 Intranet 上的用户访问并限制所有其他用户访问的情况下，可以使用此授权插件。如果认为在服务器上有违反安全的情况发生，可以快速启用此插件授权以拒绝违反安全的 IP 地址进行访问。WMS IP 地址授权插件可以对特定的发布点或对整个服务器启用。服务器和发布点授权插件将协同工作。

配置 WMS IP 授权方式是选择该选项，然后单击界面底部的 按钮，或者在这个授权选项上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 8-19 所示的对话框。在这时才可以配置允许或者拒对流式媒体服务器发布的内容的访问。具体的 IP 地址通过单击【添加 IP】按钮，在打开的如图 8-20 所示的对话框中添加。在这里既可以添加单个主机 IP 地址（选择“单台计算机”单选按钮），也可以添加一组 IP 地址（选择“计算机组”单选按钮）。

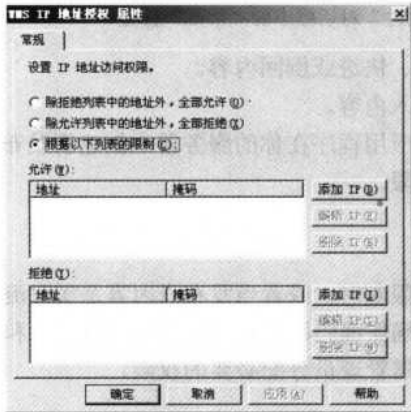


图 8-19 “WMS IP 地址授权属性”对话框中的“常规”标签

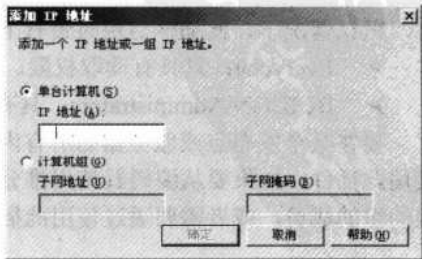





图 8-20 “添加 IP 地址”对话框



在插件属性配置中，绝大多数插件中的选项都可以继续配置其属性。配置方法与上面介绍的一样，那就是在相应选项上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令（有该时才可配置），或者在选择相应插件选项后单击配置界面底部的  按钮（呈激活状态时才可配置）打开对应的属性对话框进行。

另外，对于插件选项的启用，或禁止方法是：在相应插件选项上的状态列单击鼠标右键，如果原来为“已禁用”状态，则在弹出的快捷菜单中选择【启用】命令，或者直接在界面底部单击  按钮，均可使相应方式变为“已启用”状态，也就是启用了该插件选项；如果原来为“已启用”状态，则在弹出的快捷菜单中选择【禁用】命令，或者直接在界面底部单击  按钮，均可使相应方式变为“已禁用”状态，也就是禁用了该插件选项。

本节后面各插件选项的属性配置，以及启用或禁用方法都一样，不再赘述。

3. 使用 WMS 发布点 ACL 授权插件

此插件允许为服务器上的发布点创建访问控制列表（ACL），服务器和发布点授权插件将协同工作。可以通过如图 8-21 所示的此插件属性对话框（属性对话框的打开方法参见前面的说明，下同，不再赘述）向用户或组分配下列访问权限。

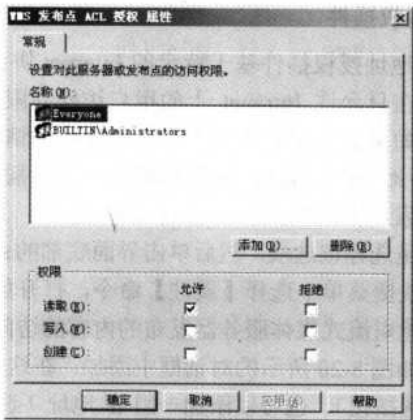


图 8-21 “WMS 发布点 ACL 授权属性”对话框中的“常规”标签

- 读取：允许用户或应用程序打开、播放、快进或倒回内容。
 - 写入：允许用户或应用程序向服务器写入内容。
 - 创建：与写入权限结合时，允许用户或应用程序在你的服务器上创建新发布点。
- 默认情况下，此插件启用时带有下列访问权限。
- Everyone：只具有读取权限。
 - BUILTIN\Administrators：具有完全权限。

要在某个发布点或服务器的所有内容上设置限制时，或者当发布点内容是实况流时，可使用此插件。如果要从编码器使用推分发，则要确保编码器管理员是同时具有写入和创建权限的组的成员，或者需要通过使用此插件向编码器管理员分配必要的权限。

注意 身份验证插件和授权插件协同工作以便授予客户端访问流式媒体内容的权限。如果启用了 WMS NTFS ACL 授权插件或 WMS 发布点 ACL 授权插件，却没有启用身份验证插件，那么单播客户端将无法访问服务器。

8.3.2 “日志记录” 插件属性配置

在如图 8-18 所示界面的“类别”列表中选择“日志记录”选项，打开如图 8-22 所示配置界面。在这里仅有一个选项需要配置，那就是“WMS 客户端日志记录”，如果启用，则可以记录通过单播流连接的播放机的活动数据。这项也将使服务器和发布点日志记录插件协同工作。

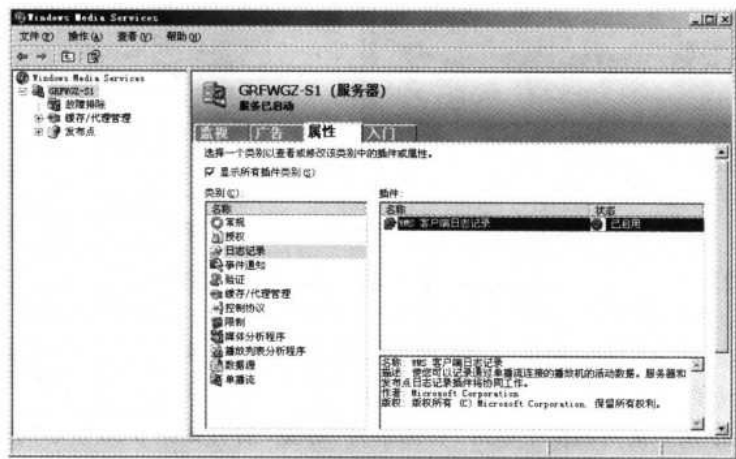


图 8-22 流媒体服务器属性窗口“日志记录”选项配置界面

双击该插件，打开这个插件的属性配置对话框，如图 8-23 所示。该插件选项的属性对话框有三个标签，在“常规”标签中可以设置日志记录的文件名和保存位置，以及日志记录的循环周期。单击【浏览】按钮可重新配置日志文件名和位置，单击【扩展】按钮以显示当前日志文件的完整路径。

日志文件默认的保存路径是%SystemRoot%\System32\LogFiles\WMS\<V>\，其中<V>表示与产生日志记录数据的发布点同名的文件夹。如果插件正在记录服务器的数据，则<V>表示[Global]文件夹。如果正在使用远程计算机进行管理，则该目录位于生成日志文件的服务器上，而不是位于管理计算机上。可使用 UNC 格式或绝对地址。

默认文件名模板是 WMS_<Y><m><d>.log，其中<Y>是年，<m>是月，<d>是日。在日志文件关闭时，该模板用于确定适当的文件名。例如，如果日志文件在 2006 年 12 月 1 日关闭，而且使用了默认文件名模板，则此时的日志文件名是 WMS_20061201.log。

可使用环境变量和通配符。环境变量必须用百分号（%）分隔开。通配符必须用小于号（<）或大于号（>）分隔开。下列字符将由下画线（_）代替：<、>、?、%、"、或*。

如果启用了“日志记录”插件，则“当前记录到”文本框中将显示活动的日志文件路径。单击如图 8-23 所示的对话框“日志循环周期”栏中的【修改】按钮，打开如图 8-24 所

在“日志条目”区域中的设置定义了哪些统计信息将被写入日志文件。如果选择了“连接到该服务器的客户端”复选项，则可以收集直接从服务器接收流的客户端的数据；如果选择了“从播放机缓存区或缓存/代理服务器播放的会话”复选项，则可以收集下级服务器的客户端活动数据；如果选择了“播放机统计信息”复选项，则可以使插件仅保存由播放机活动创建的日志；如果同时选择了“仅保存具有以下 Role 属性值的播放机统计信息”复选项，则在从播放列表传输内容时，可以根据媒体元素的 role（角色）属性来自定义要保存的播放机统计信息日志。日志记录插件的默认 role 属性是 ADVERTISEMENT，它用于将播放列表中的流标识为广告。如果使用其他 role 属性，则可在提供的空白处键入其他 role 值。

role 属性的主要用途是帮助分析和理解日志记录数据。如果使用数据库来跟踪日志记录数据，那么可以创建按类型区分内容使用情况的报告。例如，可以创建一个报告来显示已播放的音乐文件的各种类型，创建一个图表来显示用户首选的内容类型或已播放的公共服务公告的数量。例如，可以将 role 属性的值设置为 movie，然后通过分析日志文件确定电影共播放了多少次。切记，如果 media 元素引用另一个播放列表而非特定项目，那么广告计数器将不会更新。

role 属性指定 media 元素的用途或类型。可以使用此属性为数字媒体源创建自定义类别，如 music、bumper、promo 或 public service announcement。WMS 客户端日志记录插件使用 role 属性中指定的值来填充 cs-media-role 字段。

可以使用任何命名方案来设置 role 属性的值。但是，值 Advertisement 具有特殊的意义。只要服务器开始播放 role 属性值为 Advertisement 的 media 元素，“监视”标签上的“广告”计数器就会计数。通过包装播放列表播放的广告按相同的方式使计数器计数。

在下面的示例中，第一个项目采用 role 属性值 musicsegment 记录在日志中，而第二个项目则采用 role 属性值 Advertisement。第二个项目还包含设置为 true 的 noSkip 属性以禁止用户跳过该广告。

```
<?wsxversion='1.0'?>
<smil>
  <mediasrc="MusicVideo.wmv"role="musicsegment"/>
  <mediasrc="Comm11.wmv"role="Advertisement"noSkip="true"/>
</smil>
```

如果在如图 8-25 所示的对话框的“日志格式”栏中选择了“旧式”单选项，则日志格式中的 role 属性不可用。

如果在如图 8-26 所示的对话框中选择了“分发服务器统计信息”复选项，则可以使插件保存由分发服务器活动创建的日志。

8.3.3 “事件通知”插件属性配置

在如图 8-22 所示界面的“类别”列表中选择“事件通知”选项，打开如图 8-27 所示配置界面。服务器和发布点的事件通知插件也是相互协同工作的。

如果启用“WMS WMI 事件处理程序”选项，则可以通过 Windows 管理规范（WMI）无缝、安全地接收有关所有内部 Windows Media 服务器事件的通知（无论在本地计算机还是

492 网管员必读——网络应用（第2版）

远程计算机上)。通过 WMI，可以使用一个一致、基于标准、可扩展，且面向对象的接口来管理 Windows。

如果启用“WMS 动态脚本事件处理程序”选项，则可以自定义任务，例如：Windows Media 服务器如何响应内部事件、向事件授权，或响应基本插件动作（如启用或禁用插件），方法是使用脚本语言（例如，Microsoft JScript、Microsoft Visual Basic Scripting Edition 或 Perl）。

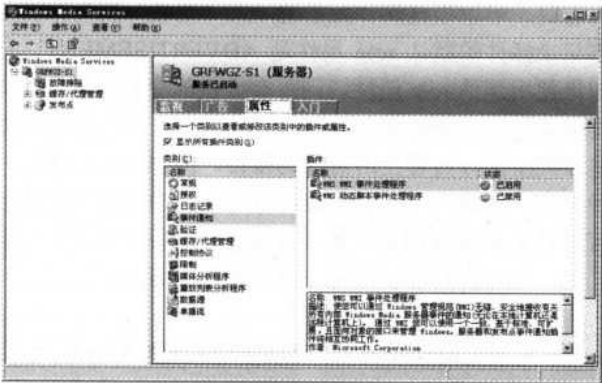


图 8-27 流媒体服务器属性窗口“事件通知”选项配置界面

“WMS WMI 事件处理程序”选项的属性对话框如图 8-28 所示。WMI 事件处理程序插件控制 Windows Media Services 报告的 Windows 管理规范（WMI）事件。可在对话框中单独选择要报告的事件，或者单击【全选】或【全部清除】按钮全选，或者全部不选。

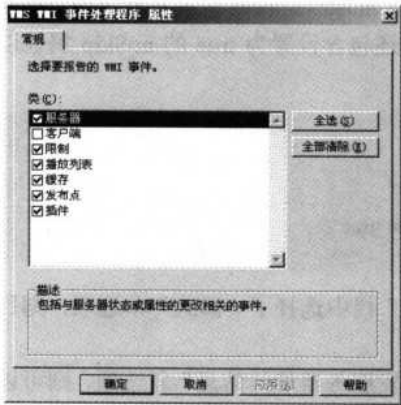


图 8-28 “WMS WMI 事件处理程序属性”对话框中的“常规”标签

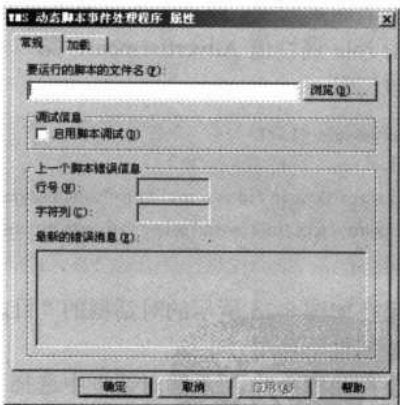


图 8-29 “WMS 动态脚本事件处理程序属性”对话框中的“常规”标签

Windows Media Services 和其他程序使用这些事件来响应服务器上的活动。因为客户端事件数量很多，而且发生很频繁，所以默认情况下，此事件处理程序不报告给它们。如果选择报告“客户端”事件，请仔细监视服务器的性能以确保处理器没有超载。也可以为此插件配置下列复选项。

- 服务器：选中此复选框，则可以报告当服务器的状态发生更改或者当更改了服务器的属性时调用的事件。
- 客户端：选中此复选框，则可以报告当客户端连接到服务器、与服务器断开连接或者更改了播放模式时调用的事件，例如，当用户快进或停止数字媒体文件时。
- 限制：选中此复选框，则可以报告当发布点或服务器的限制被修改或者已经达到时所调用的事件。
- 播放列表：选中此复选框，则可以报告与广播播放列表相关的活动所调用的事件。
- 缓存：选中此复选框，则可以报告与缓存内容相关的活动所调用的事件，例如，缓存命中或缓存未命中。
- 发布点：选中此复选框，则可以报告当发布点状态更改或者当更改了插件属性时调用的事件。
- 插件：选中此复选框，则可以报告由任何与服务器或发布点插件相关的属性所调用的事件。

“WMS 动态脚本事件处理程序属性”对话框，如图 8-29 所示。它有两个标签，其中“常规”标签允许附加自定义脚本，可以使用此脚本来提供有关 Windows Media 服务器上的事件的反馈。可以使用任何支持 Microsoft ActiveX 脚本接口的脚本语言来编写脚本，例如，Microsoft JScript、Microsoft Visual Basic Scripting Edition（VBScript）、Perl、PScript 和 Python。

在“要运行的脚本的文件名”文本框中可键入要运行的脚本文件的名称，也可以单击【浏览】按钮来定位文件。

在“调试信息”区域中设置确定是否将与脚本文件一起使用调试程序。如果选择了“启用脚本调试”复选项，则可以将 Microsoft 脚本调试程序附加到脚本文件中。如果在运行脚本时遇到错误，则调试程序将停止脚本、捕获错误、在对话框中显示错误以使用户能解决问题。



要启用脚本调试，必须在服务器上安装脚本调试程序。可以从 Microsoft 网站上的 Microsoft Scripting Technologies 界面下载 Microsoft 脚本调试程序。Microsoft 脚本调试程序对网络服务账户不起作用。要将 Microsoft 脚本调试程序与 Windows Media Services 一起使用，则必须配置 Windows Media Services 以使用本地系统账户。如果使用本地系统账户，则当使用 IP 地址引用那些要求身份验证的网络资源时，Windows Media Services 对这些网络资源只有有限的访问权限。记住将 Windows Media Services 设置成调试后，使用网络服务账户以恢复正常操作。

必须安装正确的脚本引擎才能使调试程序正常工作。默认情况下，VBScript 和 JScript 引擎与 Windows 操作系统一起安装。如果使用其他脚本语言，请确保安装了正确的脚本引擎。应该将自定义插件或第三方插件放到某个受保护的目录下以防篡改。受保护的目录可以是任一已设置成拒绝向未经授权的用户提供写入权限的目录。

WMS 活动脚本事件处理程序插件只适用于在 Windows Server 2003 Enterprise Edition 或

494 网管员必读——网络应用（第2版）

者 Windows Server 2003 Datacenter Edition 中运行的 Windows Media Services 9 系列。如果运行的是 Windows Server 2003 Standard Edition，那么此功能将得不到支持。

单击图 8-29 所示的对话框中的“加载”标签，打开如图 8-30 所示的对话框。在这里可以选择配置在服务器上加载插件的方式。在进程内加载一部分插件服务器运行起来将更快，而且对于信息请求的响应也更快。进程外插件将变慢，不过如果它们停止响应，并不会导致 Windows Media 服务器停止工作，因此在出现如服务器停机这样不可接受的风险时它们将很有用。当然也可以在进程外运行验证、授权和事件处理程序插件（作为可执行文件），而不必将它们加载在进程内（作为服务器进程的一部分）。

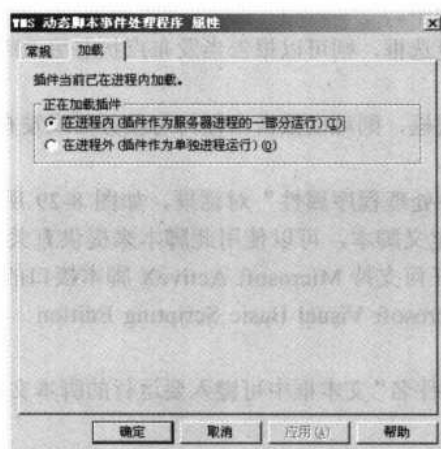


图 8-30 “WMS 动态脚本事件处理程序属性”对话框中的“加载”标签

如果选择“在进程内”复选项，则可使 Windows Media Services 服务将插件作为服务器进程的一部分来运行；如果选择“在进程外”复选项，则可使 Windows Media Services 服务将插件作为自身的进程来运行。

因为“缓存/代理管理”插件通常不安装，也不使用，所以，在此不作介绍。

8.3.4 “验证”插件属性配置

在如图 8-27 所示界面的“类别”列表中选择“验证”选项，打开如图 8-31 所示配置界面。这时可以配置用户对流式媒体内容访问时所采用的身份验证方式。

身份验证是保证运行 Windows Media Services 服务器的安全性的最基本措施。它将对试图访问 Windows Media 服务器资源的任何用户进行身份确认。Windows Media Services 包含有身份验证插件，可以启用该插件来验证用户凭据。身份验证插件与授权插件协同工作：在对用户进行身份验证之后，授权插件将控制对内容的访问。

Windows Media Services 身份验证插件分为下列两个类别。

- 匿名身份验证：此类插件不在服务器和播放机之间交换请求与响应信息，例如，WMS 匿名用户身份验证插件。
- 网络身份验证：此类插件基于登录凭据验证用户身份，例如，WMS 协商身份验证

插件。

当用户尝试访问服务器或发布点时，服务器首先尝试通过匿名身份验证插件对用户进行身份验证。如果启用了多个匿名身份验证插件，那么服务器将只使用列出的第一个插件。如果该尝试失败，或者匿名身份验证插件没有启用，那么服务器就会尝试使用网络身份验证插件对用户进行身份验证。如果启用了多个网络身份验证插件，那么服务器将尝试使用客户端也支持的第一个插件。

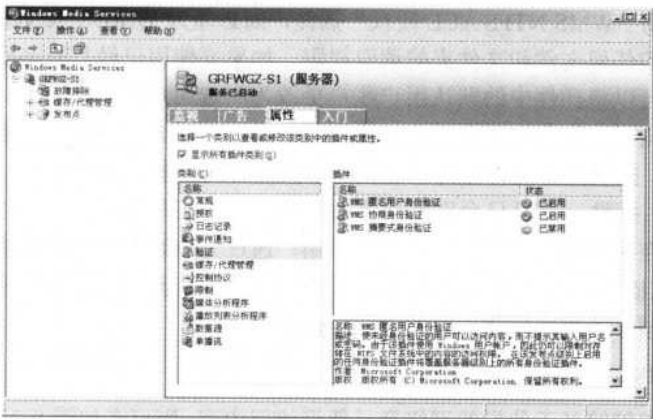


图 8-31 流媒体服务器属性窗口“验证”选项配置界面

如果启用了所有默认的 Windows Media Services 身份验证插件，那么当播放机尝试访问服务器时，服务器就会首先使用 WMS 匿名用户身份验证插件对用户进行验证。如果不能基于为该插件指定的匿名用户账户给用户访问权限，那么服务器将尝试使用 WMS 协商身份验证插件对用户进行身份验证。如果这次尝试失败，则 Windows Media Player 7 和更高版本将继续尝试使用此辅助方法进行身份验证。先前版本的播放机将在辅助方法失败一次之后停止。

如果播放机是通过 HTTP 进行连接的，那么每当用户停止、暂停、快进或者倒回内容时，播放机都会断开与服务器的连接。如果用户尝试继续接收内容，则身份验证和授权过程将再次进行。



注意

可以在服务器和发布点级别启用多个身份验证插件。如果为服务器启用了身份验证插件，然后为该服务器上的发布点启用另一个身份验证插件，那么对用户进行身份验证时将只使用发布点的插件。

身份验证插件和授权插件协同工作以便授予客户端访问流式媒体内容的权限。如果启用了 WMS NTFS ACL 授权插件，或 WMS 发布点 ACL 授权插件，却没有启用身份验证插件，那么单播客户端将无法访问服务器。

WMS 摘要式身份验证插件只适用于在 Windows Server 2003 Enterprise Edition 或者 Windows Server 2003 Datacenter Edition 中运行的 Windows Media Services 9 系列。如果运行的是 Windows Server 2003 Standard Edition，那么此功能将得不到支持。

496 网管员必读——网络应用（第2版）

1. 使用 WMS 匿名用户身份验证插件

如果希望用户未经提示输入用户名或密码即可访问内容，那么可以在如图 8-31 所示界面中启用“WMS 匿名用户身份验证”插件。这样，当用户尝试连接到 Windows Media 服务器时，该插件将使用在插件属性中指定的 Windows 用户账户对用户进行身份验证。

此插件选项的属性对话框如图 8-32 所示，在这里可以配置匿名访问的账户信息。默认情况下，在此插件中指定的用户账户是 WMUS_servername。如果要与“WMS 匿名用户身份验证”插件一起使用“WMS NTFS ACL 授权”插件，则必须为 WMUS_servername 账户提供即将从发布点播放的任何文件和文件夹的读取权限。如果要使用已经具有必要权限的另一个匿名用户账户，则可以将插件中的默认用户账户更改为所选用户账户。

当此插件启用时，将允许匿名用户连接到服务器。可以通过启用授权插件限制匿名用户可以访问的内容。授权插件允许你为内容设置不同的访问控制策略。例如，通过使用“WMS NTFS ACL 授权”插件，可以只允许用户访问发布点中的某些内容。

该插件可以在服务器上的单个发布点上启用。通过为内容文件夹设置适当的访问控制列表（ACL），可以确保此插件使用的账户只能访问特定的内容。这种情况的一个例子是同时具有免费和基于预订的数字媒体内容的 Internet 站点。

2. 使用 WMS 协商身份验证插件

如果希望用户能够基于他们的网络登录凭据访问内容，则可在如图 8-31 所示界面中启用“WMS 协商身份验证”插件。此插件使用加密的请求/响应方案对用户进行身份验证。这是一种安全的身份验证形式，因为用户名和密码不通过网络发送；播放机通过与 Windows Media 服务器进行加密信息交流来确认密码。WMS 协商身份验证插件依赖于已确立的用户登录凭据，并使用 NTLM 或 Kerberos 身份验证方法对其进行验证。

通过使用此插件，可以对各种操作系统上的用户进行身份验证。NTLM 身份验证是 Windows NT Server 4.0 中的默认身份验证方法。为了与运行 Windows NT 4.0 及更早版本的计算机兼容，在 Windows Server 2003 中仍保留了这种身份验证方法。该方法还可以用于对登录到运行 Windows 2000 Server，或更高版本的独立计算机上的用户进行身份验证。Kerberos 身份验证是 Windows 2000 Server 和 Windows XP 操作系统中使用的默认身份验证方法。

这种形式的身份验证适用于需要支持多种 Windows 客户端并为机密内容提供保护的 Intranet 站点。该插件选项没有属性配置对话框。

3. 使用 WMS 摘要式身份验证插件

如果希望通过 Internet 连接到服务器的用户在提供了用户名和密码之后能够访问内容，则可以启用“WMS 摘要式身份验证”插件。此插件使用请求/响应 HTTP 身份验证方案，该方案不需要在网络上发送密码。相反，该插件使用以哈希算法加密的密码对用户进行身份验证。此方法比基本身份验证更安全，但不如 NTLM、Kerberos 或其他私钥身份验证方案安全。当观众通过外部网络（如 Internet）进行连接，并且希望提供起码的用户身份验证时，适宜使用“WMS 摘要式身份验证”插件。

该插件选项的属性对话框如图 8-33 所示。在这里的配置选项非常简单，仅一个领域配置。领域是用来对用户和组进行身份验证的资源逻辑分组。通过对比 Active Directory 域来验证用户身份。用户名与密码与领域相关联，以便允许同一授权信息用于多个资源。

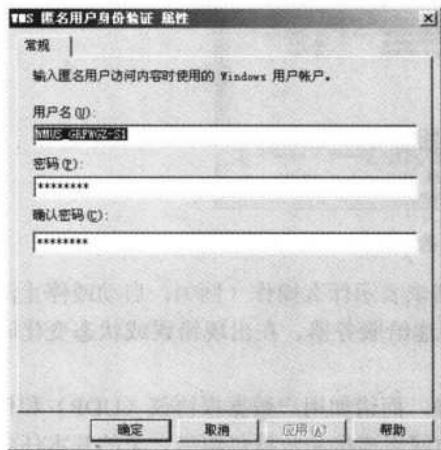


图 8-32 “WMS 匿名用户身份验证 属性”对话框中的“常规”标签

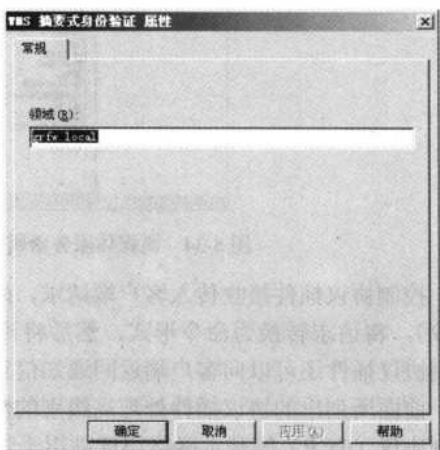


图 8-33 “WMS 摘要式身份验证 属性”对话框中的“常规”标签

要使用“WMS 摘要式身份验证”插件，则 Windows Media Services 必须是 Active Directory 域的一部分。Active Directory 域的域控制器必须是一台运行 Windows Server 2003 的计算机。



注意

Windows Media Player 9 系列或使用 Windows Media Player 9 系列 ActiveX 控件的播放机支持摘要式身份验证。尝试使用早期版本的播放机进行连接的用户将不能通过身份验证，并会收到一个拒绝访问的消息。

8.3.5 “控制协议”插件属性配置

在如图 8-31 所示界面“类别”列表中选择“控制协议”选项，打开如图 8-34 所示界面。在这里有 3 个控制协议插件选项可以配置。数据传输协议是指在两台设备之间传输数据的标准化格式。协议类型可以确定诸如错误检查方法、数据压缩方法，以及文件结束确认之类的变量。如果所有的网络都是以同一方式构建的，并且所有网络软件和设备的行为都类似，那么只需要一种协议即可处理所有的数据传输需求。而在现实中，Internet 是由数百万运行各种软硬件组合的不同网络组成的。因此，为了以可靠方式向客户端传输数字媒体内容，需要有一组设计良好的协议。

Windows Media Services 通过使用控制协议插件来管理这些协议的使用。Windows Media Services 包括 WMS HTTP、WMS MMS 和 WMS RTSP 3 个控制协议插件。除 WMS 子 HTTP 控制协议插件外，其他插件在默认情况下都是启用的。

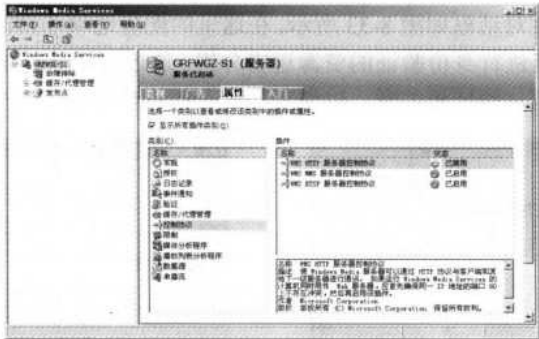


图 8-34 流媒体服务器属性窗口“控制协议”选项配置界面

控制协议插件接收传入客户端请求，确定该请求表示什么操作（例如，启动或停止流式播放），将请求转换为命令形式，然后将该命令传递给服务器。在出现错误或状态变化时，控制协议插件还可以向客户端返回通知信息。

前面所列出的协议插件处理高级别的数据交换，而诸如用户数据报协议（UDP）和传输控制协议（TCP）等基本网络协议则用于管理诸如网络连接和数据包纠错之类的基本任务。MMS 和 RTSP 协议与 UDP 或 TCP 协议一起组合使用。

图 8-35 描述了 Windows Media Services 如何使用不同的协议在 Windows Media 服务器、编码器、内容源，以及客户端之间协商连接。

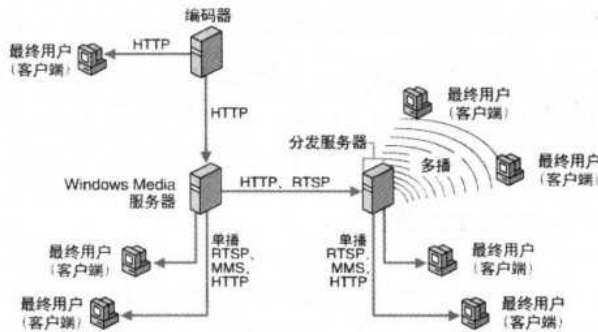


图 8-35 3 个控制协议在 Windows Media Services 中的使用

Windows Server 2003 Enterprise Edition 或 Windows Server 2003 Datacenter Edition 中的 Windows Media Services 9 系列包括下列附加的网络功能。

- 多播传输：可以从服务器上的广播发布点以多播流方式传递内容。以多播流方式接收内容的客户端不使用基于连接的协议。相反，它们通过加入多播广播来接收流。在客户端定位并加入多播流时需要的信息位于一个带有 .nsc 文件扩展名的多播信息文件中。客户端首先通过 Web 服务器或电子邮件中的链接打开该文件，然后使用其中包含的信息连接到多播流。
- 无线优化：可以使用转发纠错在流中发送额外的数据包以纠正由无线网络使用的由损耗传输方法引起的错误。

注意 在设置分发服务器（一台运行 Windows Media Services 的服务器，用于发布从另一个流式源（如编码器或其他 Windows Media 服务器）接收的内容。）使用快速流式播放功能时，请使用 RTSP 或 HTTP 协议连接到源服务器（作为内容发布起点的 Windows Media 的服务器）。

1. 使用 HTTP 协议

通过使用超文本传输协议 (HTTP)，可以将内容从编码器传输到 Windows Media 服务器，在运行 Windows Media Services 的不同版本的计算机间，或被防火墙隔开的计算机间分发流，以及从 Web 服务器上下载动态生成的播放列表。HTTP 对于通过防火墙接收流式内容的客户端特别有用，因为 HTTP 通常设置为使用端口 80，而大多数防火墙不会阻断该端口。它的使用范围可参见图 8-36 所示。可以通过 HTTP 向所有 Windows Media Player 版本和其他 Windows Media 服务器传递流。如果客户端通过 HTTP 连接到服务器，不会发生协议翻转。

Windows Media Services 使用 WMS HTTP 服务器控制协议插件控制基于 HTTP 的客户端连接。必须启用此插件才能允许 Windows Media Services 通过 HTTP 向客户端传输内容或从 Windows Media 编码器接收流。

在启用 WMS HTTP 服务器控制协议插件时，该插件会尝试绑定到端口 80。如果另一个服务，如 Internet 信息服务 (IIS) 正在使用同一 IP 地址上的 80 端口，那么就不能启用该插件。当运行 Windows Media Services 的服务器播放由 ASP 页或 Web 脚本生成的动态播放列表时，也会用到 HTTP 协议。

注意 接收 HTTP 广播流的客户端可能在流结束之后长达 90 秒的时间内不能重新连接到流。发生这种延迟的原因是 Windows Media 服务器在内容结束之后让数据路径保持打开状态，以便接收日志记录数据。

“WMS HTTP 服务器控制协议 属性”对话框如图 8-37 所示。在这里要设置可以使用 HTTP 控制协议的服务器 IP 地址和所用的 HTTP 协议端口。

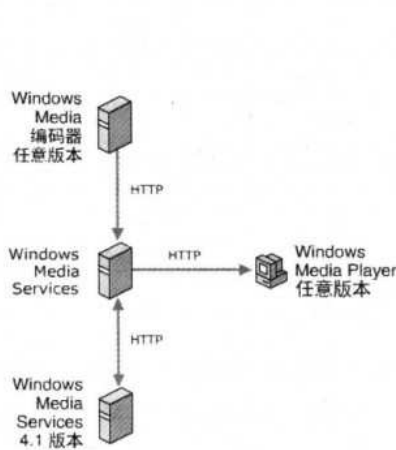


图 8-36 HTTP 控制协议的使用

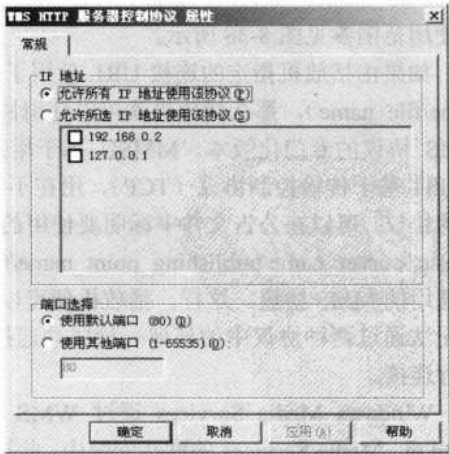


图 8-37 “WMS HTTP 服务器控制协议 属性”对话框

在“IP 地址”栏中的设置决定了控制协议如何使用服务器上的 IP 地址。如果选择了“允

500 网管员必读——网络应用（第2版）

许所有 IP 地址使用该协议”复选项，则允许服务器上的所有 IP 地址在传输内容时都使用 HTTP 控制协议；如果选择了“允许所选 IP 地址使用该协议”复选项，则仅允许在“IP 地址”列表中选择的那些 IP 地址在传输内容时使用 HTTP 控制协议。如果已在服务器上创建了多个 IP 地址，则此选项很有用。

在“端口选择”区域中的设置决定了控制协议使用的端口。如果选择了“使用默认端口”复选项，则使用默认的 HTTP 传输端口 80；如果选择了“使用其他端口”复选项，则可指定其他端口使用 HTTP 传输，然后在下面的文本框中键入要使用的端口。



对该插件所作的更改将只应用于新的客户端连接请求，已经连接到服务器的客户端不受影响。因为默认情况下 Windows Media Services 和像 IIS 这样的 Web 服务都尝试绑定到端口 80，所以在一台服务器上同时使用这两种服务可能会导致冲突。要避免端口冲突，可以将 Windows Media Services 指派到其他端口，或者创建其他 IP 地址，以便每个服务都可以在单独的 IP 地址上使用端口 80。

如果在具有多个网络接口卡的 Windows Media 服务器上启用了服务器控制协议插件，则可通过在“允许所选 IP 地址使用该协议”列表中选择 IP 地址来防止其使用某个协议。如果选择了“允许所选 IP 地址使用该协议”单选项，但是却没有选择任一系列出的 IP 地址，则所有 IP 地址都可以使用该协议。如果不允许任何 IP 地址使用该协议，则应当禁用此服务器控制协议插件。另外，Windows Media Services 已启用了 IPv6 协议。

2. 使用 MMS 协议

Microsoft Media 服务器（MMS）协议是 Microsoft 为 Windows Media Services 的早期版本开发的专有流式媒体协议。在以单播流方式传递内容时，可以使用 MMS 协议。此协议支持快进、倒回、暂停、启动和停止索引数字媒体文件等播放机控制操作。如果要支持使用 Windows Media Player 早期版本的客户端，需要使用 MMS 或 HTTP 协议满足其流请求。它的使用范围参见图 8-38 所示。

如果由播放机指定的连接 URL 使用了 MMS（例如 `mms://server_name/publishing_point_name/file_name`），那么播放机就可以使用协议翻转协商使用最佳协议。MMSU 和 MMST 是 MMS 协议的专门化版本。MMSU 基于用户数据报协议（UDP），是流式播放的首选协议。MMST 基于传输控制协议（TCP），用在不支持 UDP 的网络上。如果需要强制服务器使用特定的协议，可以在公告文件中标明要使用的协议，用户还可以在内容地址中指定协议（例如，`mmsu://server_name/publishing_point_name/file_name`）。为了利用协议翻转，建议在 URL 中使用通用的 MMS 协议。这样，播放机便可以使用 MMSU 或 MMST 协议连接到流。如果播放机无法通过两种协议中的任何一种成功连接到流，则会尝试使用超文本传输协议（HTTP）进行连接。

Windows Media Services 通过 WMS MMS 服务器控制协议插件实现 MMS 协议。在 Windows Media Services 的默认安装中，此插件是启用的，并且绑定到 TCP 端口 1755 和 UDP 端口 1755。

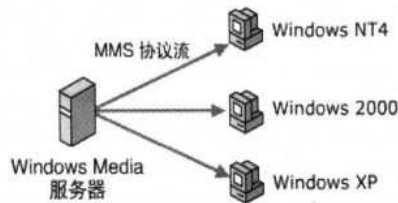


图 8-38 WMS MMS 服务器控制协议的使用范围

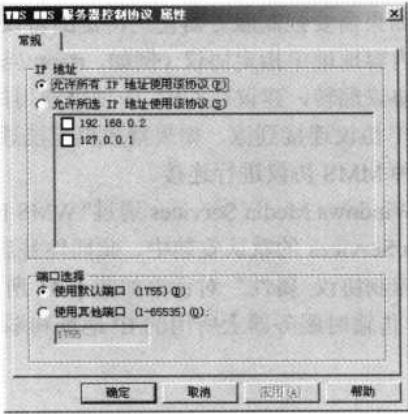


图 8-39 “WMS MMS 服务器控制协议 属性”对话框中的“常规”选项卡



一些 ISA 客户端可能会在连接到端口 1755 时遇到麻烦。为纠正此问题，请创建一个名为 Wspcfg.ini 的文件并将其保存到名为 %SystemRoot%\Windows\System32\Windows Media\Server 的文件夹中。文件中应包含如下文本。

```
[WMServer]
LocalBindTcpPorts=1755
LocalBindUdpPorts=1755
```

“WMS MMS 服务器控制协议 属性”对话框如图 8-39 所示。在这里如果在服务器使用 IP 地址和端口，同样可以设置 WMS MMS 服务器控制协议插件。

在“IP 地址”区域中的设置决定了控制协议如何使用服务器上的 IP 地址。如果选择了“允许所有 IP 地址使用该协议”复选项，则允许服务器上的所有 IP 地址在传输内容时都使用 MMS 控制协议；如果选择了“允许所选 IP 地址使用该协议”复选项，则仅允许在“IP 地址”列表中选择的那些 IP 地址在传输内容时使用 MMS 控制协议。

在“端口选择”区域中的设置决定了控制协议使用的端口。如果选择了“使用默认端口”复选项，则使用默认的 MMS 传输端口 1755；如果选择了“使用其他端口”复选项，则可指定其他端口使用 MMS 传输，然后在下面的文本框中键入要使用的端口。

3. 使用 RTSP 协议

可以使用实时流式传输协议（RTSP）以单播流方式传递内容。这是一个应用程序级别的协议，是为控制实时数据（如音频和视频内容）的传递而专门创建的。此协议是在面向纠错的传输协议基础上实现的，支持停止、暂停、倒回及快进索引 Windows Media 文件等播放机控制操作。可以使用 RTSP 将内容传输到运行 Windows Media Player 9 系列或 Windows Media Services 9 系列的计算机。RTSP 是一个控制协议，该协议与数据传递实时协议（RTP）依次发挥作用，实现向客户端提供内容。RTSP 控制协议的使用范围参见图 8-40 所示。

如果连接 URL 中使用了 RTSP（例如，rtsp://server_name/publishing_point_name/file_name），那么 RTSP 会自动协商内容的最佳传递机制。然后该协议指示 RTP 协议使用 UDP 协议传递流式内容，或者在不支持 UDP 的网络上使用一种以 TCP 协议为基础的协议进行传递。

如果需要强制服务器使用特定的协议，可以在公告文件中标明要使用的协议。用户还可以在内容地址中指定协议（例如，`rtspu://server_name/publishing_point_name/file_name`）。为了利用协议翻转，建议在 URL 中使用通用的 RTSP 协议。这样，播放机便可以使用 RTSPU 或 RTSPT 协议连接到流。如果播放机无法通过任意一种 RTSP 协议成功连接到流，则会尝试使用某种 MMS 协议进行连接。

Windows Media Services 通过“WMS RTSP 服务器控制协议”插件实现 RTSP。在 Windows Media Services 的默认安装中，此插件是启用的，并且绑定到 TCP 端口 554。“WMS RTSP 服务器控制协议 属性”对话框如图 8-41 所示。在这里同样可以设置用于控制从服务器进行的 RTSP 传输时服务器上所用的 IP 地址和端口。

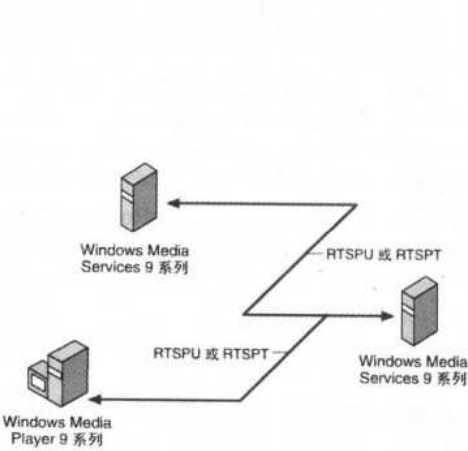


图 8-40 RTSP 协议的使用范围



图 8-41 “WMS RTSP 服务器控制协议 属性”对话框中的“常规”标签

在“IP 地址”区域中的设置决定了控制协议如何使用服务器上的 IP 地址。如果选择了“允许所有 IP 地址使用该协议”复选项，则允许服务器上的所有 IP 地址在传输内容时都使用 RTSP 控制协议；如果选择了“允许所选 IP 地址使用该协议”复选项，则仅允许在“IP 地址”列表中选择的那些 IP 地址在传输内容时使用 RTSP 控制协议。

在“端口选择”区域中的设置决定了控制协议使用的端口。如果选择了“使用默认端口”复选项，则使用默认的 RTSP 传输端口 554；如果选择“使用其他端口”复选项，则可指定其他端口使用 RTSP 传输，然后在下面的文本框中键入要使用的端口。

4. 协议翻转的工作原理

在前面三个控制协议的介绍中，都提到了“协议翻转”，那它是如何实现的呢？

Windows Media Services 依据客户端的具体环境为其选择适当协议的能力称为协议翻转。如果要支持多种客户端版本，支持通过防火墙连接的客户端或通过不同类型的网络连接的客户端，那么协议翻转将很有用。如果服务器上所有可用的服务器控制协议插件（包括 WMS HTTP 服务器控制插件）都已启用，那么协议翻转的效果会达到最佳。

Windows Media 服务器使用协议翻转的目的是为了与客户端建立最佳的连接。客户端在尝试连接服务器时，会发送有关自身类型及能支持哪些协议的信息。Windows Media 服务器

将该信息与已启用的协议进行比较，然后使用适用于当时情况的最佳协议。通常，服务器和客户端之间的第一次连接尝试是成功的，不需要采取进一步行动。如果该连接请求不成功，那么客户端将尝试使用其他可支持的协议连接到服务器。在每一次协议翻转尝试期间，客户端都会经历一段非常短暂、通常不易察觉的延迟时间。

此外，在客户端尝试与服务器建立新的连接时，将会优先选用客户端在前一次连接中使用的协议。如果让客户端通过公告访问内容，那么 MMS 协议将被自动采用，从而确保在必要时进行协议翻转。

在此建议使用协议翻转，以确保客户端享受到最佳的流式播放体验。如果客户端使用带有 mms://前缀的 URL 连接到流，那么协议翻转将在必要时进行。请注意，用户可以在播放机的属性设置中禁用协议。如果播放机只支持一个协议，那么翻转就无法进行。协议翻转中使用的具体逻辑取决于连接服务器的客户端类型。在 Windows Media Player 9 系列中采用如图 8-42 所示的翻转原理。



图 8-42 Windows Media Player 9 系列的协议翻转原理

当 Windows Media Player 9 系列或者使用 Windows Media Player 9 系列 ActiveX 控件的播放机尝试通过带有 mms://前缀的 URL 连接到服务器时，服务器会自动使用 RTSP。如果服务器上启用了“快速缓存”（所有新发布点的默认情况），那么服务器将首先尝试通过 RTSPT（采用基于 TCP 的传输方式的 RTSP）连接到客户端。如果播放机不支持该协议，那么服务器将尝试使用 RTSPU（采用基于 UDP 的传输方式的 RTSP）进行连接。如果该连接也不成功，则在启用了 WMS HTTP 服务器控制协议插件的情况下，服务器将尝试使用 HTTP 协议进行连接。如果没有启用快速缓存，那么在连接客户端时，服务器将首先尝试使用 RTSPU，然后使用 RTSPT，最后使用 HTTP 协议进行连接。

早期版本的播放机所采用的协议翻转原理如图 8-43 所示。



图 8-43 早期版本的播放机的协议翻转原理

Windows Media Player 的早期版本，如 Windows XP 中的 Windows Media Player，不支持 RTSP 协议。然而，MMS 协议为这些播放机提供了协议翻转支持。因此，当早期版本的播放

机尝试使用带有 mms://前缀的 URL 连接到服务器时，服务器将自动为播放机协商最佳的协议。服务器将首先尝试使用 MMSU（采用基于 UDP 的传输方式的 MMS）连接到客户端。如果播放机不支持该协议，那么服务器将尝试使用 MMST（采用基于 TCP 的传输方式的 MMS）进行连接。如果该连接也不成功，则在启用了 WMS HTTP 服务器控制协议插件的情况下，服务器将尝试使用 HTTP 协议进行连接。

注意 当分发服务器尝试连接到源服务器时，不使用协议翻转。分发服务器不能使用带有 mms://前缀的 URL 来请求连接到源服务器。如果分发服务器尝试使用 RTSP 进行连接，那么该请求将被转换为 RTSPU。如果必须采用或需要优先使用基于 TCP 的传输方式，那么 URL 中必须使用 rtsp://前缀。如果服务器必须使用 HTTP 进行连接，那么 URL 必须使用 http://前缀。

如果 Windows Media 服务器与客户端之间被不能传递 UDP 数据包的防火墙或代理服务器隔开，则应在 WMS 单播数据写入器插件属性中禁用 UDP 数据包传输。试图通过未启用 UDP 的网络组件接收 UDP 传输内容的客户端可能会在协议翻转过程中遇到延迟。

8.3.6 “限制” 插件属性配置

在如图 8-34 所示界面“类别”列表中选择“限制”选项，打开如图 8-44 所示界面。在这里列出了许多具体可使用的发布点限制选项。要设置相应选项，只需在相应的选项中选择“值”列中的复选框，然后在后面的文本框中输入具体的限制值即可。

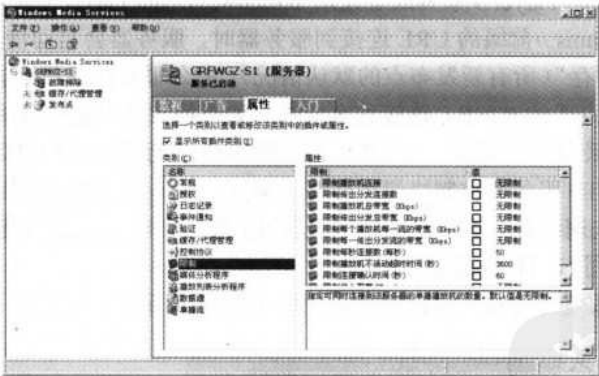


图 8-44 流媒体服务器属性窗口“限制”选项配置界面

- 以下是列表中各限制选项的简要说明。
- 限制播放机连接：设置播放机连接的最大数量。
 - 限制传出分发连接数：设置可以连接到此源服务器的分发服务器的最大数量。
 - 限制播放机总带宽：指定播放机连接可以使用的最大带宽量（以 Kb/s 为单位）。
 - 限制传出分发总带宽：指定分发服务器连接可以使用的最大带宽量（以 Kb/s 为单位）。

- 限制每个播放机每一流的带宽：指定单个播放机连接可以使用的最大带宽量（以 Kb/s 为单位）。
- 限制每一传出分发流的带宽：指定单个分发服务器连接可以使用的最大带宽量（以 Kb/s 为单位）。
- 限制每秒连接数：指定每秒处理的连接请求最大数量。默认值是 50。
- 限制播放机不活动超时时间：指定播放机自动断开前保持连接但处于不活动状态中的秒数。默认值是 86 400 秒（24 小时）。这个默认值使用户可以将内容的播放暂停相当长的一段时间，而且无须重新连接到服务器即可重新启动播放。
- 限制连接确认时间：指定在断开连接之前服务器等待播放机响应连接确认请求的时间是多少秒。连接确认请求由服务器发送给播放机，用以验证到播放机的连接。默认值是 60 秒。如果要在延迟时间很长的环境中传输内容，请考虑增大该值以适应网络条件。
- 限制每个播放机的“快速启动”带宽：指定单个播放机可用来加速流式内容的初始缓冲操作的带宽量（以 Kb/s 为单位）。
- 限制快速缓存内容传递速率：（只用于点播发布点）限制流式内容的加速系数并控制另外有多少带宽可用于将内容传输到播放机的本地缓存中。

当达到某个限制时，后续连接请求将被拒绝，并在“疑难解答”事件列表中会显示一个达到限制的事件。如果为发布点设置的限制超出为服务器设置的限制，则服务器限制将覆盖发布点限制。

8.4 部署 Windows Media Services 服务器

有很多方案可以部署 Windows Media Services，通常有实况产品演示、交互电视节目和电影、实时消费者新闻发布会、重大新闻事件、宽带视频存储和交互训练演示。一旦某部分内容可通过 Internet 获得，可发现这一内容并对其发出请求的客户端的数量将是巨大的。对部署进行计划时，需要知道对内容的请求过多时服务器将出现什么反应。下面是评估部署时应该记住的一些要求。

1) 可扩展性

Windows Media Services 通过设计之后具有了可扩展性，可支持一定范围的部署，范围从具有数百个连接请求的小型 Internet 电台到生成数百万个请求的大规模的流式媒体网站。可管理服务器组和发布点组，也可以管理单个的服务器和发布点。

2) 安全

用户可能希望保护 Windows Media 服务器上的某些内容的安全，以便只允许某些特定的客户端进行连接。Windows Media Services 支持多种验证和授权方法，使用户可控制对内容的访问。

3) 流质量

如果连接到服务器的客户端增加，则其可用的带宽可能会减少。另外，服务器上的负载可能超过处理器处理内容的能力。如果正在传输视频内容，那么请使用多比特率视频对编码进行调试，以确保带宽可按照需要进行放大或缩小。

8.4.1 Windows Media Services 服务器部署概述

本节描述了 Windows Media Services 的实际应用和部署概述。Windows Media Services 技术广泛适用且易于配置，因此，几乎可在任何情况下用于实现适宜的流式媒体解决方案。任何流式媒体项目都有三个阶段：项目计划、汇集与管理内容和协调内容分发。除这三个阶段外，还有许多初始的防范措施及后续步骤，用以改进流式媒体过程。

基于 Windows Media 技术的流式媒体系统一般都包括运行编码器（如 Windows Media 编码器）的计算机、运行 Windows Media Services 的服务器和大量运行播放机（如 Windows Media Player）的客户计算机。编码器可将实况的和预先录制的音频、视频内容转换成 Windows Media 格式。Windows Media 服务器通过网络或 Internet 来分发内容，然后由播放机接收内容。它们之间的关系如图 8-45 所示。

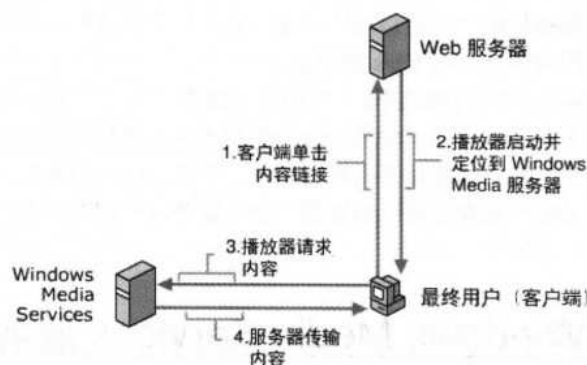


图 8-45 Windows Media 服务器、Windows Media 编码器和播放机之间的关系

在典型的用户方案中，用户单击网页上的链接来请求内容。然后 Web 服务器将请求重定向到 Windows Media 服务器，并启动用户计算机上的播放机。此时，Web 服务器不再参与流式媒体传输过程，这是因为 Windows Media 服务器与播放机建立了直接连接，并已开始将内容直接传输给用户。

Windows Media 服务器可从多种不同的源接收内容。预先录制的内容可以存储在本地服务器上，也可以从联网的文件服务器上提取。实况事件则可以使用数字录制设备记录下来，经编码器处理后发送到 Windows Media 服务器进行广播。Windows Media Services 还可以重新广播从远程 Windows Media 服务器上的发布点传输过来的内容。

有效的流式媒体部署要求成功管理以下三个主要因素：观众可以使用的带宽、网络或 Internet 连接的容量，以及内容的流式播放要求。

第一个因素是观众，这也是最重要的因素。观众可以使用的带宽在决定提供的内容类型和质量方面起着关键作用。带立体声的大型高清晰度视频流需要的带宽超出使用标准拨号调制解调器进行连接的客户端的可用带宽。此外，还应该知道观众的规模。即使是少量的高速流，也可能影响一般的商业网络或 Internet 网关的性能。

第二个因素是网络容量评估。像局域网（LAN）这样的计算机网络在特定时间内传输的数据量是有限的。网络中的每个连接都将占用网络的一部分容量。当传输中的数据总量接近

网络极限时，单个数据连接的速度将开始下降。在计划流式媒体部署时，请确保网络容量远大于内容的带宽要求。

第三个因素的内容是最灵活多变的。无论是音频还是视频，内容质量的提高都将导致带宽要求的增加。使用质量提高方法（如多比特率编码或可变比特率编码）可以显著改变必需的带宽量。实况和预先录制的内容经编码处理后才能播放给观众。在该处理过程中作出的选择对于可以触及的观众范围和必需的带宽大小有重大影响。

8.4.2 部署过程中需要考虑的问题

流式媒体部署工程并不一定困难。在所有的部署方案中，都必须作出某些基本的选择。在进行选择时，应考虑以下因素：有待分发的数字媒体内容的具体类型、观众的特征，以及用于传递内容的设备。

1. 流式播放实况内容或预先录制的内容

可使用 Windows Media Services 来播放实况内容或预先录制的内容。不过，对于不同的（实况的或预先录制的）内容，开发流式播放解决方案时使用的方法会有某些差别。

1) 实况内容

可使用多种方法获得实况内容。可将实况捕获设备（如麦克风或数字摄像机）连接到正在运行编码器（如 Windows Media 编码器）的计算机上，并且后者应通过网络与 Windows Media 服务器相连。还可以用同样的方式将其他数字媒体播放设备（如视频和 CD 播放机）连接到编码计算机上，以便基于录制的资料创建实况广播。

因为用户无法控制实况内容的播放，所以一般情况下实况内容以广播流（而非点播流）方式播放。另外，应该为编码器和服务器之间的网络连接分配一定量的带宽，并且要避免其他网络通信的干扰。

在实况广播过程中，因为内容只是在服务器的内存缓冲区中留存一小段时间，所以系统不太可能从流式播放错误中恢复。可使用转发纠错在播放过程中提供纠错处理，而无须强制播放机向服务器请求纠错信息。如果希望用户在广播结束后仍可以获得内容，则可以考虑对广播进行存档，以便该内容可以重新广播出去或者以点播方式提供给用户。

2) 预先录制的内容

预先录制的内容是最容易管理和设置的内容类型。一般情况下此类内容采用预先编码的数字音频或视频，可以通过播放机（如 Windows Media Player）进行呈现。可以播放单个文件或多个文件，也可以创建播放列表文件对内容进行组织，从而为用户提供连贯的播放效果。

默认情况下，可以在 Windows Media Services 中使用下列文件类型。括号内是这些文件的文件扩展名。

- 高级系统格式文件（.asf）：这些文件是可以包含多种元素（如视频、音频、脚本命令、HTML 和元数据）的 Windows Media 文件，而且可使用任何编解码器对其进行编码。
- Windows Media 音频文件（.wma）：这些数字媒体文件采用高级系统格式，并使用 Windows Media 音频编解码器来进行编码。一般说来，这些文件是音频文件，尽管其中也包含脚本、图片和源数据。

508 网管员必读——网络应用（第2版）

- Windows Media 视频文件（.wmv）：这些数字媒体文件采用高级系统格式，并使用 Windows Media 视频编解码器来进行编码。一般说来，这些文件是视频文件，尽管其中也包含脚本和其他指令。
- MP3 文件（.mp3）：这些数字媒体文件使用动画专家组（MPEG）的音频格式。
- JPEG 文件（.jpeg 或 .jpg）：这些文件是根据“联合摄像专家组”标准确定格式的图像文件。
- 多播信息文件（.nsc）：这些文件是 Windows Media 元文件，可将客户端定位到多播广播。使用这些文件的目的是为播放机（如 Windows Media Player）定义多播流属性。
- 客户端播放列表文件（.asx、.wax 和 .wvx）：这些文件是 Windows Media 源文件，用做客户端播放列表，并由服务器用做客户端重定向器。其中包含可供播放机（如 Windows Media Player）使用的指令和引用。
- 服务器端播放列表文件（.wsx）：这些文件是用做服务器端播放列表的 Windows Media 元文件。其中可以包含音频、视频和图像文件的组合。

还可以使用 Windows Media Services 9 系列 SDK 来创建自定义媒体分析程序以支持其他文件类型。



MP3 文件不能使用 Windows Media Services 中的智能流式播放功能。另外，如果启用了适当的媒体分析程序插件，则可从 Windows Media 服务器播放其他数字媒体文件格式。媒体分析程序插件将文件中包含的信息转换成与 Windows Media 服务器和播放机兼容的格式。

如果预先录制的内容存储在网络源中而非本地服务器上，那么请确认服务器是否具有网络访问权限，以及是否能够及时检索到内容。一般情况下不会出现这方面的问题，原因在于服务器无须呈现内容，因而能够以较高的数据速率检索预先录制的内容。

播放预先录制的内容时，应当确定需要创建哪种类型的用户播放效果。预先录制的内容可使用点播与广播两种发布点来播放。

2. 选择单播分发或多播分发

单播和多播是流式媒体分发的两种不同形式。基于观众的特征和内容的类型，每种形式都有各自的优点与缺点。

1) 单播

单播流是服务器和客户端之间的一对一连接，这意味着每个客户端都接收不同的流，且只有那些请求流的客户端才接收流。以单播流方式传递内容时既可以采用点播发布点，又可以采用广播发布点。

单播流式传输是 Windows Media 服务器用来传递内容的默认方法。它由 WMS 单播数据写入器插件自动启用，在默认情况下处于启用状态。

如图 8-46 所示，是显示通过使用点播发布点以单播流方式传递内容的示例。

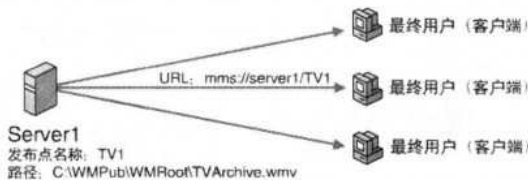


图 8-46 单播方式示例

在如图中名为 Server1 的 Windows Media 服务器上有一个名为 TV1 的点播发布点，该发布点标识要传输的内容的位置，内容可在本地服务器或网络文件系统中安置，可以将特定文件、播放列表文件或目录作为来源。在例中，发布点将存储在本地 Server1 上的播放列表文件作为来源。当准备让用户开始传输时，可创建一个为用户提供指向内容的 URL 的公告。因为内容是以单播流方式传递的，所以每个播放机都有一个到 Server1 的唯一连接。

单播流的优点包括：播放机和服务器之间的互动性、设置便捷，以及支持多比特率流式播放功能。但是，单播流用户的数量受到内容比特率和服务器网络速度的限制。单播观众过多将使网络或服务器无法承受。在下列情况下，请考虑使用单播流。

- 希望采用多比特率编码和智能流式播放。
- 网络与服务器的容量可以承受预计中的观众规模与内容比特率。
- 需要详细的客户端日志记录。
- 网络没有启用多播方式。

2) 多播

多播流是指 Windows Media 服务器和接收流的客户端之间的一对多关系。利用多播流，服务器向网络上的一个多播 IP 地址传输，客户端通过向该 IP 地址订阅来接收流。所有的客户端都接收相同的流。因为无论有多少个接收流的客户端，服务器只传输一个流，所以多播流需要的带宽量与包含相同内容的单个单播流的带宽量相同。使用多播流会节省网络带宽，且对于带宽较低的局域网可能非常有用。

以多播流方式传递内容时只能采用广播发布点。另外，网络路由器必须已启用多播，这意味着它们可以传输 D 类 IP 地址。如果网络路由器未启用多播，仍可以通过局域网的本地网段以多播流方式传递内容。

如图 8-47 所示，是显示通过使用广播发布点以多播流方式从编码器分发内容的示例。下面介绍的是图中所示的多播编码器的实况内容传输的步骤：

(1) 将实况图像从数字摄像机发送到运行 Windows Media 编码器的计算机上的视频捕获卡。图像被编码成 Windows Media 格式，然后使用 HTTP 传输到服务器。

(2) 在名为 Server1 的 Windows Media 服务器上，使用“添加发布点向导”添加将编码器作为来源的广播发布点。作为向导的一部分，可以选择允许进行单播翻转。单播翻转确保不能访问多播流的播放机仍可以通过切换到可用的单播流来接收内容。例如，如果网络路由器未启用多播，或者如果播放机超出了多播流的生存时间 (TTL) 范围，则播放机可能无法访问多播流。

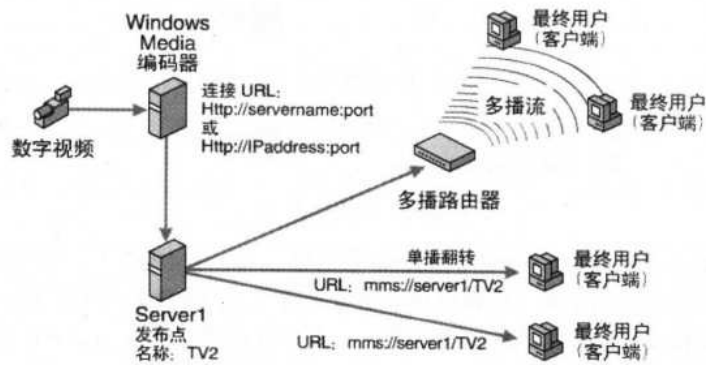


图 8-47 多播方式示例

(3) 使用“多播公告向导”创建一个公告以便向用户提供指向内容的 URL。使用该向导可创建一个多播信息文件（文件扩展名为.nsc）、一个公告文件（文件扩展名为.asx）、在网页中嵌入公告所需的代码或者三个选项的任意组合。



注意

多播流式播放和 WMS 多播数据写入器插件只适用于在 Windows Server 2003 Enterprise Edition 或者 Windows Server 2003 Datacenter Edition 中运行的 Windows Media Services 9 系列。如果运行的是 Windows Server 2003 Standard Edition，那么这些功能将得不到支持。

多播传输在服务器与客户端之间创建一对多的关系。服务器广播单个的流，然后用户可以在广播过程中访问该流，用户无法控制内容的播放。多播流对服务器和网络的要求较低，但需要对网络进行修改以便多播网络通信和常规网络通信能够和谐共存。在下列情况下，请考虑使用多播流。

- 正在向大批观众广播内容，而网络带宽和服务器容量有限。
- 网络启用了多播方式。

8.4.3 容量计划

容量计划的目的是确保内容可到达所有用户而没有延迟或中断。通过对流式媒体网络进行适当的计划和配置，可以改善响应时间、数据吞吐量、内容可用性并减小数据错误率。

容量计划基于三个变量：观众数量、内容的类型和大小，以及服务器的数量和速度。在大多数情况下，容量计划用于确定向指定的观众群提供定量的内容时所需的服务器要求，当然在某些环境下，可以针对三个变量中的任意一个制订计划。

可以通过使用如下等式来估计所需的网络容量：
所需的网络容量 = 内容比特率×估算的客户端数量
容量计划中涉及多个方面，本节的以下主题分别对这些方面进行了介绍。

1. 评估流式内容

随着内容的画面大小和分辨率的增加，对服务器的要求也在增加。请确定内容的使用方式和使用环境。是否正将内容分发给大范围的观众？如果是，那么应该尽量减小文件大小。

观众是否会使用多种连接速度来访问内容？如果是，则可能需要对内容进行多比特率编码。要为每个用户确定带宽要求的粗略估算值，需将文件大小除以播放时间（以秒为单位）。例如，2 兆字节（MB）的数字媒体文件代表大约 16 000 000 比特。如果内容长度大约是 11/2 分钟，则平均比特率为 180Kb/s。大多数拨号调制解调器无法传输超过 56Kb/s 的信息，这意味着使用电话线访问流的客户端将必须在播放开始之前等待播放机缓冲文件，否则将只能接收到断断续续的视频和音频。

2. 估算观众数量

即使不觉得所有的用户会同时请求内容，也必须容许使用量出现峰值。同时应该考虑到用户连接速度，因为其中的差距可能很大。要估算观众数量，需要确定流式播放过程中并发用户的最大值。例如，某公司计划通过局域网（LAN）向全部 10 000 名员工提供联机培训。过去的培训实践表明最多只有 5%的员工在任一指定的时间同时访问培训内容。因此，网络必须能够将内容可靠地传递给 500 个并发用户。

3. 计算所需的服务器容量

使用估算出的带宽要求和观众数量来确定网络和服务系统为满足要求而必须具备的容量。要估算所需服务器容量的总量，请用估算出的观众数量乘以单个用户所需的比特率。特定服务器的实际容量随计算机的不同而不同。就常规而言，具有 256MB 内存的单处理器（233MHz）计算机（运行 Windows Media Services）最多可以支持 1 000 个 28.8Kb/s 的单播流。表 8-1 说明了以上最低配置情况下，在用户数量和内容比特率增加时，服务器容量需求的增加情况。

表 8-1 最低服务器配置下，用户数量和内容比特率增加时的服务器容量需求增加

流的比特率（Kb/s）	网络连接类型	每台服务器并发用户的数量
28.8（实际上是 20）	电话调制解调器	1200
56.6（实际上是 33）	电话调制解调器	600
100	ISDN	300
300	DSL/电缆/LAN	100

例如，如果以 300Kb/s 的比特率将联机培训内容传递给 500 个并发用户，则服务器系统和网络必须能够处理每 150Mb/s 的数据量。如果服务器仅是满足 256MB 内存的单处理器（233MHz），运行 Windows Media Services 的计算机，则至少需要 5 台（实际上是至少需要 6 台，因为 5 台是按服务器的最大处理能力计算的）这样的 Windows Media 服务器才能处理这么大的数据量。

4. 评估增长潜力

一段时间后，观众的数量可能会增加，而且内容可能会翻倍。需要据此评估长期的流式媒体计划，并调整所需容量的计算值。可能影响流式播放开销的一些其他因素包括安全功能及其他服务，如自动内容复制和负载平衡软件。

随着越来越多的人使用服务器，并发连接的数量很可能增加。请留意系统的上限，并考虑哪种对策适用于部署状况。例如，需要考虑是否能够支持 50%的增长潜力、25%的增长潜力，否则系统容量将成为部署中的环境限制。

512 网管员必读——网络应用（第2版）

5. 组合所需的容量

估算好内容的带宽要求、观众数量和期望的服务器容量，并确定了预期的增长率之后，即可建立服务器系统并对当前网络作必要的更改以适应服务器的容量。

下面概述了升级服务器和网络容量的一些有效技术。

- 将单 CPU 服务器升级为多 CPU 服务器。
- 安装额外的网卡或者升级服务器网卡，以支持更高带宽的网络连接。
- 添加额外的 Windows Media Services 服务器，并采用负载均衡程序，以便创建更大的逻辑服务器用于网络上的流式媒体。
- 在网络各处分布缓存/代理服务器，并采用内容复制程序，以便拉近内容与客户端之间的距离，降低对原始内容服务器的某些要求。
- 将负责处理流式媒体请求与传输的网络交换机设置成全双工模式，以维护不间断的信息流。

6. 测试容量

部署流式媒体解决方案之前，应当执行负载测试以确保装配好的服务器系统可以支持必要的内容及观众，并且运行状况达到预期效果。

可在一台或多台客户计算机上运行 Windows Media Load Simulator 9 系列以模拟任意数量的客户端连接。还可以配置负载模拟器，以重新创建多种客户端行为，包括连续播放内容、播放多比特率内容、浏览和定位点播内容，以及通过身份验证进行连接。每个负载模拟器都可以向服务器加载 1 000 个以上的并发连接，用这种方法同时测试网络上限和服务器的上限，具体情况取决于计算机的速度。应当模拟足量的并发负载，以便模拟 Windows Media 服务器上的峰值负载，与此同时监视服务器，看是否超出了某项限制。Windows Media Load Simulator 9 软件可以向微软购买。

8.4.4 执行负载均衡和群集化

根据以上部署考虑和测试结果，可以采用多种技术来优化流式播放过程、提高系统可靠性，以及收集有关系统、内容和观众的有用信息。

群集化是通过使用一组计算机（或称群集）而非单一计算机来确保关键服务的可用性。群集中的每台计算机都称为一个节点。群集化允许从服务中删除一个或多个节点而不妨碍系统的运行，因而这种方法提高了系统的容错性和可扩展性。群集化通常作为更大的负载均衡过程的一部分；在负载均衡过程中，内容请求被传播到各个节点以便平均分布工作负载。群集化的基本结构如图 8-48 所示。

群集中的每个节点都为该组提供了一批特定的资源。Windows Media Services 可能只是特定节点上的可用资源之一，而且并不是指定群集上的所有节点都安装了 Windows Media Services。如果某节点出现故障或者关闭，那么群集化软件将把服务器要求重新分配给群集中具备适当可用资源的其他成员，该过程称为故障转移。常见的故障转移模式有下面两种。

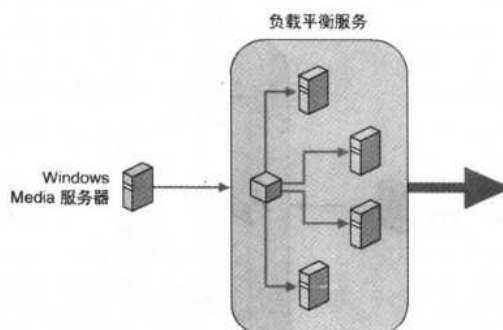


图 8-48 基本服务器群集结构

- 级联故障转移：出现故障的节点中的资源将被平均分配到群集中的其他节点。此模式假定群集中的所有其他节点都具有一定的额外容量。
- $N+1$ 故障转移：出现故障的节点中的资源将被重定向到某个留作备用的后备节点上。此模式假定群集中全部或大部分的多余容量都分配给了一个节点。

当故障节点或脱机节点恢复时，群集化软件可以自动将一部分，或全部已重新分发的资源移回原来的位置。要提供有效的故障转移保护，群集中的每个节点都必须直接连接到内容源。内容源可以是编码器、发布点或文件服务器。

除了控制故障转移外，群集化软件还允许管理员将这些节点作为单一系统（而非独立的计算机）加以控制和管理。

网络负载均衡群集是在 Windows Server 2003 中提供的一种服务器群集化方法。每个群集都可以在一个逻辑 Internet 名称下支持多达 32 台计算机。群集将自动检测服务器故障或状态的变化情况，并将请求重定向到剩余的服务器上，从而使用户感觉运行从未间断。

负载均衡软件一般使用群集化软件来管理群集内的服务器工作负载，以便在节点间平均分配工作负载。它监视每个节点的运行情况，并根据预设的公式或算法来分配流式媒体工作负载。同时它还确保，即使流来自多个不同节点中的任意一个，内容也将由同一个 IP 地址来表示。如图 8-49 所示的是群体服务器中都正常工作时的负载分配图示。

主要的负载均衡策略有下面两种。

- 基于硬件的负载均衡：也称为反向代理，此方法依赖于网络中位于服务器群集和客户端之间的代理服务器。反向代理服务器接收客户端的流请求，然后将客户端重定向到适当的服务器，或者为客户端代理该服务器中的内容。为避免创建单个的故障点，可以同时使用两个或多个反向代理计算机。
- 基于软件的负载均衡：基于软件的负载均衡产品，例如，Microsoft Network Load Balancing，将一定比例的服务器总负载分配给群集中的每一个节点。负载均衡软件在群集的每一个节点上运行，并根据每一台服务器承担的总工作负载的百分比来计算下一个接受新请求的节点。这种负载均衡方法的优点包括速度、可配置性、可靠性和较低的成本。

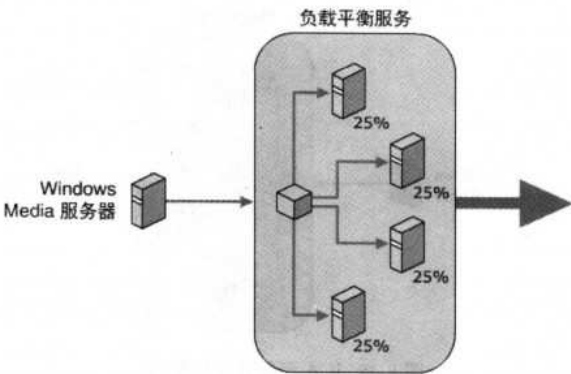


图 8-49 正常情况下群集中节点的负载分配图示

网络负载均衡是在 Windows Server 2003 中提供的，它采用一种完全分布式的筛选算法。群集中的所有节点每秒钟都发出包含自身状态信息的“心跳”信号。网络负载均衡软件将监视这些信号以了解群集状态的变化情况，并适当调整服务请求的分发。当群体中有节点出现故障时，该节点上的原来的负载会自动转移到其他正常工作的节点上，一般以平均摊分，如图 8-50 所示就是在图 8-49 所示状态中一个节点出现故障后所出现的负载分配图示。

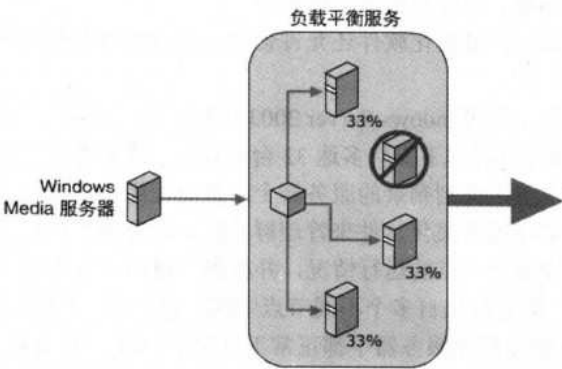


图 8-50 一个节点出现故障后的负载分配图示

8.4.5 了解可扩展性

可扩展性描述了在维持系统可靠性的同时向系统中添加组件或从系统中删除组件的难易程度。随着观众的增多，可能需要添加服务器以免需求的增加导致系统过载，或者可能希望将大型服务器系统分解成多个小的、更专用的系统。不管是哪种情况，都必须分别解决软件和硬件的可扩展性问题。

1. 软件可扩展性

Windows Media Services 的设计具备可扩展性，能够支持各种部署方案：从具有上百个连接请求的小型 Internet 电台到生成数百万个请求的大型流式媒体网站。Windows Media Services 管理单元使你既可以管理单个的服务器和发布点，也可以管理服务器和发布点组。

2. 硬件可扩展性

在 Windows Media Services 环境下，可扩展性主要指向系统中添加或从系统中删除单个的服务器。当连接数或内容的增加导致系统无法承受时，通过向系统中添加服务器可以大大改善系统性能。系统中必需的服务器数量取决于内容的比特率、内容类型和并发客户端连接的数量。

使用多个服务器时，通过某种形式的负载平衡来防止某一台服务器过载是很重要的。服务器还应该在性能和能力方面较好地匹配以确保负载平衡方法收到最大成效。单一 Windows Media Services 系统中组合使用的服务器数量不受限制。

8.4.6 了解容错

在播放数字媒体内容时，容错是指流式媒体系统在出现系统故障后维持服务，或者（起码做到）恢复服务的能力。系统错误导致故障的可能性也是系统容错性的衡量标准之一，此外还可以根据系统可用性，或者系统正常运行的时间比例来衡量容错性。

流式媒体系统只不过是内容源延伸到消费者的一条组件链。像一条链一样，每个组件都必须恰当地执行分配到的任务，否则系统本身将失败。流式媒体系统中的任何位置都可能发生错误。对 Windows Media Services 而言，上级错误是指与内容源（如编码器或数字媒体库）有关的错误，而下级错误是与向客户端分发内容有关的错误，如分发服务器或缓存/代理服务中的错误。流式媒体系统的上级组件与下级组件的关系如图 8-51 所示。

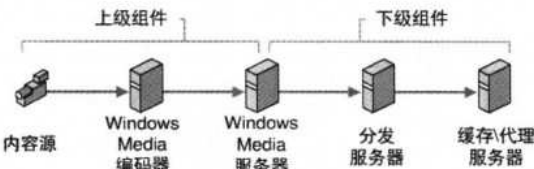


图 8-51 流式媒体系统的上级组件与下级组件的关系

流式媒体系统中容错的关键问题是冗余性。在媒体分发过程的任一阶段中，依赖于单个组件的系统就容易发生故障。

1. 上级错误

Windows Media Services 的输入错误，无论是源自编码器、远程发布点还是文件服务器，都将是严重的挑战，因为系统管理员可能不会意识到问题的存在。当上级内容源出现故障，或者断开连接时，错误将被写入“疑难解答”选项卡和会话日志中，但是 Windows Media Services 中没有明显的出错迹象。

可以通过为发布点使用多个内容源来降低发生上级错误的风险。多内容源可以由冗余编码器或备用内容文件构成，以便在主内容源不可用时供发布点使用。多内容源的流式媒体系统结构如图 8-52 所示。

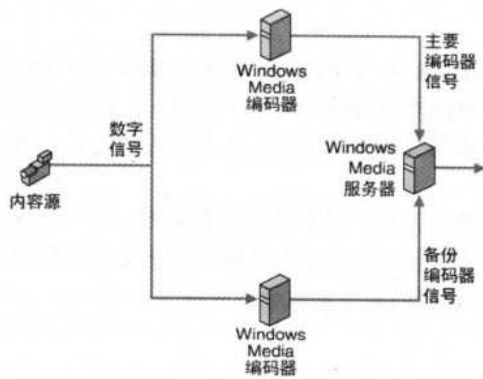


图 8-52 多内容源的流式媒体系统结构

2. 下级错误

Windows Media 服务器或某一个下级组件（如分发服务器）发生的错误可以导致客户端无法接收到请求的内容。使用多个 Windows Media 服务器来播放同一内容（称为群集化）可以减小服务中断的风险。群集化（参见图 8-53 所示）是一种有价值的容错技术，这是因为某一台服务器容量降低，或者出现故障不太可能导致整个系统的中断。如果其中一台服务器停止响应，那么该故障服务器的工作量将迅速而流畅地传输给其他服务器。

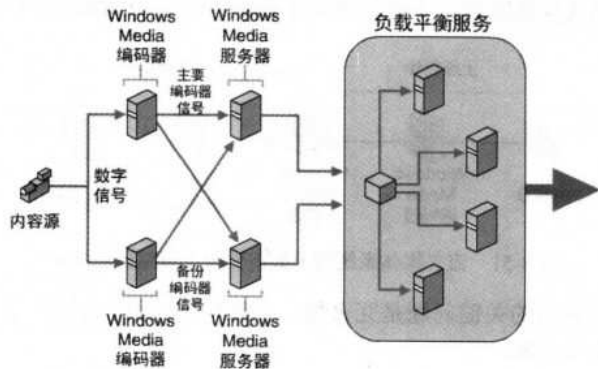


图 8-53 群集化的下级错误解决方案示例

8.4.7 监视服务器性能

监视服务器系统性能的能力对于执行有效管理至关重要。通过监视性能，可以做到以下几个方面。

- 充分发挥服务器的性能。
- 评价内容对观众的价值。
- 评估观众使用模式与倾向。


1. 使用性能监视器

Windows Media Services 中包含一个实时图形界面的性能监视器，用来观察服务器和发

布点的行为，如图 8-54 所示。图形显示说明了选择的性能数据随时间的变化情况。此外，Windows Media 性能监视器还具有各种可配置的性能计数器。



图 8-54 Windows Media Services 的图形界面性能监视器

单击图 8-54 所示界面底部的  按钮，就可打开如图 8-55 所示的动态性能监视窗口，在其中可以添加必要的性能监视计数器。

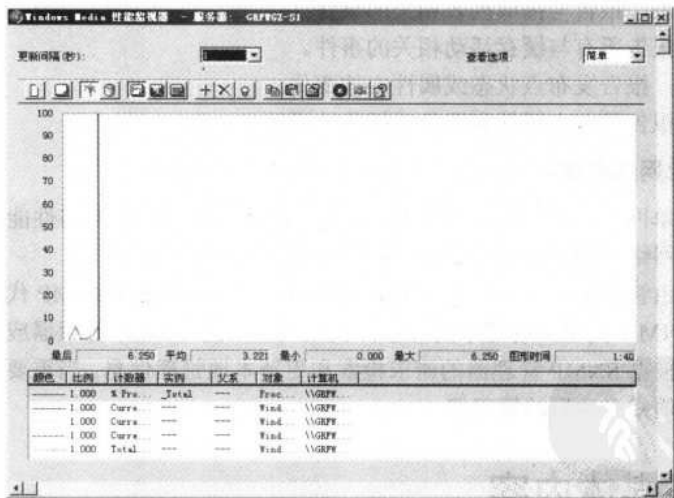



图 8-55 “Windows Media 性能监视器”窗口

添加新的性能监视计数器的方法是在如图 8-55 所示窗口中单击左上角的  按钮，打开如图 8-56 所示的对话框。

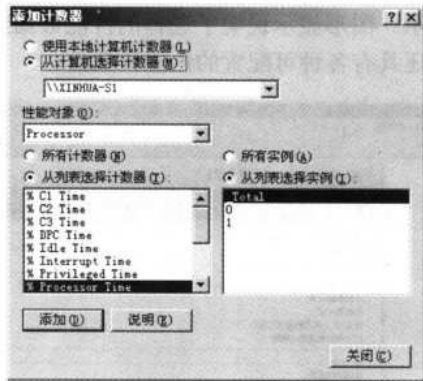


图 8-56 “添加计数器”对话框

2. 使用 WMS WMI 事件处理程序插件

此插件（参见图 8-27 所示）能够监视服务器运行状况的特定方面。启用并配置了 WMS WMI 事件处理程序插件后，即可接收关于服务器事件的本地或远程通知。在它的属性对话框中（参见图 8-28 所示）可以监视下列服务器功能。

- 服务器：报告服务器状态或属性更改。
- 客户端：报告 Windows Media Player 中的客户端事件。
- 限制：更改服务器限制或达到服务器限制时发送报告。
- 播放列表：报告与播放列表相关的事件。
- 缓存：报告所有与缓存活动相关的事件。
- 发布点：报告发布点状态或属性中的变化。
- 插件：报告发布点插件和服务器插件的活动。

3. 使用简单网络管理协议

可以使用简单网络管理协议（SNMP）来配置远程设备、监视网络性能、审核网络使用情况，以及检测网络错误或不适当的访问。

SNMP 使用由管理器和代理组成的分布式结构：管理器生成对 SNMP 代理应用程序的查询并接收来自 SNMP 代理应用程序的对象；代理响应来自 SNMP 管理器应用程序的查询。SNMP 代理负责根据 SNMP 管理器的请求检索和更新本地管理信息，当重要事件或陷阱发生时，代理还可以通知已注册的管理器。

8.5 发布媒体内容

Windows Media Services 使用发布点将客户端对内容的请求转换为安置该内容的服务器上的物理路径。在客户端成功连接到发布点之后，Windows Media 服务器管理该连接，并传输该内容。

8.5.1 添加发布点

服务器上的发布点列在控制台树中，如图 8-57 所示。通过在该左边导航栏中单击某个发布点，可以在细节窗口中修改或查看它的设置。通过在控制台树中单击“发布点”节点，可以在详细窗口中查看现有发布点的列表，还可以执行基本任务，如添加、配置或删除发布点。



图 8-57 Windows Media Services 窗口的发布点

当安装 Windows Media Services 时，广播和点播发布点会自动安装。可以按原样使用这些原始的发布点、按照自己的需要修改它们或者删除它们并添加自己的发布点。点播发布点被指定为默认设置。连接到 Windows Media 服务器的客户端通常必须将服务器和发布点名称用做地址的一部分。如果未提供发布点名称，则 Windows Media 服务器将把请求定向到默认发布点。

如果要添加新的发布点，则可在“发布点”节点上单击鼠标右键，在弹出的快捷菜单中选择【添加发布点（向导）】或者【添加发布点（高级）】命令之一，前者是以向导方式创建的，而后者则是以属性对话框配置方式创建的。向导方式除了收集这个主要信息以外，还帮助配置发布点。例如，利用该向导，你可以创建公告文件、创建包装播放列表、向播放列表中添加媒体元素，以及在该向导完成后立即启动广播发布点。对于高级用户，如果要创建简单的发布点，则“添加发布点（高级）”对话框可能比该向导快，在此仅以高级方式进行。

在选择了【添加发布点（高级）】命令后，打开如图 8-58 所示的对话框。在这里要配置一些基本的发布点属性配置，具体如下。

在“发布点类型”区域中要选择发布点是广播类型还是点播类型。广播类型就是前面介绍的“多播”方式，为实况事件时选择此选项，例如，聊天、电台节目和电视节目。用户是被动的参与者，即服务器管理员可以控制内容播放。通过此选项可以使用多播传输来保持网络带宽。

“点播”类型就是前面介绍的“单播”方式。在提供像单个的歌曲、自定义播放列表存档广播内容和基于计算机的训练这样的内容时，选择此选项。用户是主动的参与者，即他们可以按照需要控制流，也可以对内容进行启动、停止、暂停、快进或倒回等操作。此选项要求进行内容的单播传输。

记住一定要在“发布点名称”文本框中键入新的发布点名称。该名称将成为客户端用来

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

520 网管员必读——网络应用（第2版）

访问内容的 URL 的一部分。请使用有意义的名称，如要从发布点传输的内容的类型（例如，“音乐 CD”），该名称不区分大小写。

在“内容的位置”文本框中输入内容的绝对路径，可以是文件，也可以是目录。如果不熟悉具体的路径，可单击【浏览】按钮，打开如图 8-59 所示的对话框进行选择。如果选择的是目录，则要单击【选择目录】按钮。它是发布点内容的来源，可以是文件、文件的目录、播放列表、来自编码器的流、远程 Windows Media 服务器上的发布点或本地发布点。必须指定源的位置和名称。例如，可以将文件的目录指定为%systemdrive%\Wmpub\Wmroot 或 \\RemoteServer\Wmpub\Wmroot。



图 8-58 “添加发布点”对话框



图 8-59 选择源位置对话框

配置以上基本选项后，就可利用高级配置方法添加新的发布点了，如图 8-60 所示。在添加发布点之后，可以配置发布点属性，并进一步修改发布点设置。“监视”、“源”、“广告”、“公告”和“属性”标签包含用来进行修改和查看设置的工具。



图 8-60 添加了新的发布点后发布点界面

通过在新建的发布点上单击鼠标右键，在弹出的快捷菜单中还可以针对发布点执行下列任务。

1) 复制发布点

通过复制发布点，在同一台服务器上创建包括原始发布点的所有设置（如源路径、插件配置和属性设置）的副本。要复制发布点只需在相应发布点上单击鼠标右键，在弹出的快捷菜单中选择【复制】命令即可，该功能可帮助更高效地设置系统。例如，如果打算针对服务器上所有的发布点实施相同的策略，但是希望为每个发布点指定不同的源，则可以创建基本设置的副本，然后更改每个副本上的源。

2) 重命名发布点

发布点的名称是客户端用来连接到发布点的地址的一部分。要重命名发布点只需在相应发布点上单击鼠标右键，在弹出的快捷菜单中选择【重命名】命令即可。如果要重命名发布点，请切记将需要更新引用旧名称的公告文件和网页。

3) 删除发布点

当不再需要发布点时，最好删除它，以免与更新的发布点混淆。要删除发布点只需在相应发布点上单击鼠标右键，在弹出的快捷菜单中选择【删除】命令即可。当你删除发布点时，只删除发布点及其设置。不删除或更改源内容，如文件、目录、播放列表和任何相关的数据（如公告文件和日志文件）。



注意

当命名发布点时，避免使其名称与 Windows Media 服务器上的目录同名。与目录同名的发布点可能会影响将该目录作为源位置的其他发布点。

服务器并不使用用户账户访问文件夹和其他资源，默认情况下它使用 Network Service 账户。如果将 C:\WMPub 及其子目录之外的某个位置作为来源，请确保共享该文件夹，且 Network Service 账户对该文件夹至少具有读取权限。如果 Network Service 账户对某个文件夹不具有权限，则服务器将无法从该文件夹传输内容。

多播流式播放和 WMS 多播数据写入器插件只适用于在 Windows Server 2003 Enterprise Edition 或者 Windows Server 2003 Datacenter Edition 中运行的 Windows Media Services 9 系列。如果运行的是 Windows Server 2003 Standard Edition，那么这些功能将得不到支持。

8.5.2 配置发布点

本节将介绍可以使用的方法，以及在配置发布点时可修改的属性。

1. 内容源

发布点是客户端通过其建立连接以接收流的入口。源是指客户端可从发布点接收的内容所在的位置，可以向发布点指派任意一种类型的源，如文件、文件的目录、内容播放列表或来自编码器的实况流。它的属性配置在发布点的“源”标签中，如图 8-61 所示。单击其中的【更改】按钮可重新配置发布点的源位置。

可以创建用于 Windows Media Services 的动态内容来源。动态源通常是由客户端代理创建的播放列表并用于点播发布点。内容源的范围可通过使用自定义的数据源插件进一步扩展。Windows Media Services SDK 使能够创建和自定义数据源插件以满足自己的需要。



图 8-61 发布点配置界面“源”标签

2. 流式属性

在如图 8-60 所示“属性”标签上，可以更改属性设置，并添加用于修改发布点如何传输内容的插件。发布点属性影响发布点的运行方式，而插件可向发布点添加功能。Windows Media Services 将几种最常用的插件作为安装程序的一部分包括在内。其他插件可通过使用 Windows Media Services SDK 创建，也可以从第三方供应商获得。在这里所列的插件属性与本章前面介绍的流式媒体服务器的属性配置方法差不多，在此只介绍一些不同的插件选项及属性配置方法。

下面介绍“播放列表转换”插件选项，如图 8-62 所示。它是用于控制传输目录或播放列表中内容的顺序的。在其上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开如图 8-63 所示的对话框。在这里要选择一种播放方式，如果选择了“循环播放”复选项，则按目录或播放列表的顺序重复，直到被管理员停止；如果选择了“无序播放”复选项，则按随机顺序播放目录或播放列表的内容。这两个复选项可同时选择，这样系统会自动比较两种方式，以当前最容易实现的方式进行播放。



图 8-62 发布点配置界面“播放列表转换”选项配置界面

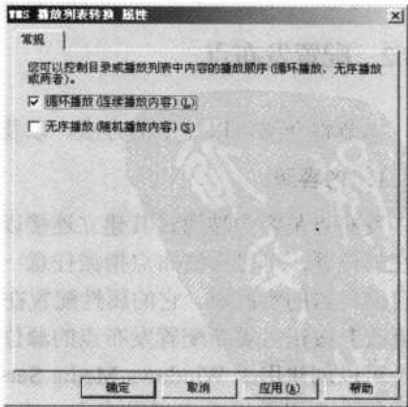


图 8-63 “WMS 播放列表转换属性”对话框中的“常规”标签

如图 8-64 所示的是“缓存/代理”插件选项的配置界面。在这里可以指定在检查源服务器上是否有更新之前，缓存/代理服务器（或在本地缓存内容的播放机）可访问被缓存内容或对广播进行流拆分操作的时间长度。在其上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，可以打开如图 8-65 所示的对话框。在其中可以设置缓存内容过期的时间。



图 8-64 发布点配置界面“缓存/代理”选项配置界面

如图 8-66 所示的是“凭据”插件选项的属性配置界面。在这里可以使分发服务器能够响应来自源服务器的验证请求。在其上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，可以打开一个对话框。在其中可以设置分发服务器向源服务器请求时的验证凭据。如果没有分发服务器，则不用配置。



图 8-65 “缓存过期属性”对话框中的“常规”标签



图 8-66 发布点配置界面“凭据”选项配置界面

3. 客户端日志记录

可在发布点启用日志记录以捕获有关连接到单播和多播流的客户端使用情况的信息。日志可用于几种不同的目的，如广告客户反馈、疑难解答和订户账单。要记录有关单播客户端的数据，需要启用 WMS 客户端日志记录插件。多播日志记录由 Windows Media Internet 服务器应用程序编程接口（ISAPI）扩展（wmsiislog.dll）提供。

日志记录在流式媒体系统中非常重要：客户端活动日志和服务器活动日志能够记录下从服务器播放了哪些内容，以及播放给谁了；日志信息可以帮助跟踪服务器的使用情况，并估计出什么时候可能需要为系统增加更多资源；可以帮助规划安全措施，如果系统受到“拒绝服务”攻击，那么日志文件可以帮助确定在攻击中使用了哪些客户端；可以通过提供对应于常见问题的事件代码帮助标识使用流式系统时用户报告的问题；可以提供历史数据，用于满足趋势分析和商业案例的需要。

WMS 日志记录插件创建的日志文件是由空格分隔的文本文件，遵循万维网联合会（W3C）日志文件标准。日志文件中的所有条目都对应于某个服务器或客户端事件，并具备对应的结果代码。默认情况下，由 WMS 客户端日志记录插件创建的日志文件保存在 %SystemRoot%\System32\LogFiles\WMS，由“多播与广告日志记录代理”创建的日志文件保存在 %SystemRoot%\System32\LogFiles\WMS_ISAPI。如果在驱动器上没有足够的磁盘空间用于写入日志文件，则日志记录插件停止记录并将一个警告消息粘贴到疑难解答列表中。

4. 安全

可以通过配置和启用一个，或多个与安全有关的插件来控制对发布点的访问。授权和身份验证插件对发布点安全具有最直接的影响，但是可另外采取多种措施来提高发布点的安全，还可以通过对客户端连接设置限制来控制访问。通过限制流式播放活动（如客户端连接的数量或每个客户端所使用的带宽）的某些方面，还可以限制恶意攻击对发布点性能产生的影响。

配置好后，如果要查看新建发布点或者其他发布点的类型、当前连接状态，可在如图 8-66 所示界面左边导航栏中单击“发布点”节点，在右边详细信息窗口中就会列出各发布点的类型、内容源位置、连接状态信息，如图 8-67 所示。



图 8-67 “发布点”节点窗口

8.5.3 从发布点进行流式播放

在已经创建并配置发布点之后，客户端可以连接到发布点并传输内容。客户端可通过使用下列方法之一来获取发布点的 URL，并通过使用该 URL 来查找内容。

客户程序（如 Windows Media Player）可通过使用发布点的 URL 来直接连接到单播发布点。例如，在 Windows Media Player 中，用户可在“打开 URL”对话框中键入该 URL。URL


由协议类型、流式媒体服务器名（如果是在互联网上，则为域名）和发布点名称组成。如果发布点将文件的目录作为来源，则还可以指定具体的文件名。如 `mms://my_server/my_pub_pt/my_file.wmv`，通过使用 MMS 协议，或由使用协议翻转逻辑的服务器选择的协议，传输 My_Server 服务器上 My_Pub_Pt 发布点中的 My_File.wmv 文件。

如果要从广播发布点传输内容，必须使用下面的 URL 格式：`<protocol>://server_name/publishing_point_name`。

在从点播发布点进行流式播放时，使用的 URL 格式随内容源不同而不同。可使用表 8-2 找出发布点应使用的播放机 URL。

表 8-2 点播发布点可使用的 URL 格式

内 容 源	URL	描 述
任何内容	<code>mms://server_name/publishing_point_name</code> 、	请求所有内容。如果以目录为源，那么此 URL 包括子目录
	<code>mms://server_name/publishing_point_name/*</code>	
	或 <code>mms://server_name/publishing_point_name/*.*</code>	
目录	<code>mms://server_name/publishing_point_name/ *.content_file_name_extension</code>	请求带有特定的文件扩展名（如 .mp3 或 .wma）的所有数字媒体文件
目录	<code>mms://server_name/publishing_point_name/ *.playlist_file_name_extension</code>	请求所有带有特定扩展名（如 .wsx）的播放列表
目录	<code>mms://server_name/publishing_point_name/ subdirectory/content_file_name</code> 或 <code>mms://server_name/publishing_point_name/ subdirectory/playlist_file_name</code>	请求特定的文件，如 <code>mms://server1/publishing_point1/movie1.wmv</code>



注意

可使用星号（*）通配符替换整个文件名（例如 *.wma），或替换文件名和扩展名（如 *.*）。在该表提供的示例中，如果使用了星号（*）作为通配符或者在发布点名称之后未指定任何东西，那么必须启用 WMS 目录播放列表分析程序插件和“允许使用通配符对目录内容进行访问”属性。如果这两者中的某一个没有启用，那么就会给客户端返回一个错误消息。

在连接到来自默认发布点的流时，客户端应使用的 URL 格式取决于将默认发布点设置为点播发布点还是广播发布点，具体情况如下所示。

- 如果默认发布点是点播发布点，则请使用适于点播发布点的任何有效语法。请求的内容必须在 URL 中明确指出，如 `mms://server_name/filename.wmv`。
- 如果默认发布点是广播发布点，则请使用格式 `mms://server_name/*` 或 `mms://server_name/*.*`，该格式将请求发布点引用的所有内容。如果发布点以目录为源，那么此 URL 包括子目录。

8.6 内容管理与制作

出于各种因素，不同项目的内容管理方法与优先级也各不相同。这些因素包括观众的人口统计特征、内容类型及可用的设备，等等。本部分分为实况内容与预先录制内容两大类讲

述了内容管理问题。因为广告内容可以用多种不同的方法提供，所以将其与其他内容类型分开讨论。

对于任何复杂的项目，计划都是首要任务。鉴于流式媒体项目的运作必须准确无误，而其部署方式又多种多样，因而进行有效的计划是至关重要的。

8.6.1 预先录制的内容概述

预先录制的内容由数字媒体文件组成。要进行流式播放（streaming）和播放（playback），数字媒体文件需具备正确的格式。可根据需要配置运行 Windows Media Services 的服务器，使其播放单个文件或者多个文件。

可使用播放列表来帮助管理预先录制内容的分发，方法是使用单个播放列表文件指向任意数量或类型的数字媒体文件。创建播放列表后，可使用它们将内容配置成所希望的方式播放。

数字媒体文件格式有很多，但不是所有格式都可以通过 Windows Media Services 来播放。在某些情况下，必须首先将数字媒体文件转换成兼容的格式才能进行流式播放。

1. 计划预先录制的内容

可根据系统容量和观众方的容量来计划和开发内容，尽可能在整个编码和流式播放过程中保留内容的原始质量。预先录制内容的计划过程与实况内容的计划过程有很大不同。

例如，如果流式音频文件的比特率对于观众的带宽容量而言过高，则流在播放过程中将被强制暂停以便播放机可以缓冲内容。如果比特率太低，则声音质量将受到影响。对编码过程进行细微调整（如从立体声切换到单声道声音）可以减小所需的流式播放比特率（甚至可以降为原来的一半），而不会影响声音的质量。

还可能遇到这样的情况，即需要向带宽状况差别很大的观众群传输内容：一些观众在局域网（LAN）内，一些使用的是数字用户线（DSL），而另外一些则通过拨号调制解调器进行连接。对内容进行细致的准备可将内容同时传输到所有这些观众，并且尽量为每个用户提供最佳效果。

1) 音频

可通过 Windows Media Services 以 Windows Media Audio（WMA）、ASF 或 MP3 格式来播放音频内容。准备内容时需要将音频内容转换（或编码）为上述某种文件格式。

尝试播放音频内容时需要考虑带宽问题。高质量的立体声广播可能很容易超出标准拨号调制解调器的容量。在编码过程中可以调整音频录制的多个可配置组件，以便在数据传输速率和音频质量之间找到适宜的平衡点。最好试验一下编码过程以便找出最佳设置组合。

如果音频内容来自多个不同的源，那么可能会发现内容的质量不能始终保持一致。在从一个内容文件过渡到下一个文件时，请尽量保持音频流畅而不间断。

2) 视频

尝试播放视频内容时，数字媒体内容比特率的重要性显得更加突出了。为了避免在播放过程中出现长时间的延迟、间隙或扭曲，视频流式播放比特率应当适应观众方的设备带宽（通常是有限的）。

视频只不过是一系列称为帧的静止图片的快速显示。每一帧都必须显示一定量的细节或

分辨率，以便准确呈现目标。提高帧分辨率可以显示更多细节。每秒显示的帧数称为帧速率。增加帧速率可以使视频中的动作显得更加流畅。流的比特率由视频的帧速率和分辨率共同决定。两种参数都可以在编码过程中加以修改，以便达到用户需要的理想比特率。

通过高速的 Internet 连接或者局域网（LAN），可以很容易地实现高分辨率视频的顺畅播放。速度极快的网络可以呈现能与 DVD 质量相媲美的视频和音频内容，但是如果通过一般的电话线进行连接，那么不经过很长时间的缓冲就无法实现高质量的视频流式播放。无论使用的是哪种连接类型，都可以通过在视频制作和编码过程中使用下列技术来为观众改善播放效果。

- 尽量减少移动：数字媒体流不是发送视频中每一帧的整个图片，而只是突出相邻两帧之间的差异。如果差异很小，则比特率可以保持在较低水平。在创建视频内容时，请尽量减少目标、摄像机和背景的移动，以便减少此后需要传输的信息量。
- 保持制作方案简捷：通常可通过减小拍摄场景的复杂度来降低视频帧呈现所需的比特数。与在彩色或不规则背景下拍摄目标相比，在普通背景下拍摄目标所需的数据传输量更少。如果视频质量比音频质量更重要，也可以在编码过程中牺牲一部分音频质量来换取视频质量的提高。
- 使用 Windows Media Services 的智能流式播放功能：可将编码器设置成以多种不同的比特率对数字媒体进行编码。这样，不管用户使用什么类型的连接，Windows Media 服务器都可以发送已针对相应比特率进行优化的流。



MP3 文件不能使用 Windows Media Services 中的智能流式播放功能。

2. 存储内容

只有在管理大量的数字媒体文件时，内容存储才成为真正需要关注的问题。在很多情况下，可以在服务器本身的某个目录下存储所有相关的数字媒体文件。当内容库不断增大时，可能需要开发单独的文件存储与管理解决方案。在存储内容方面需要考虑以下几个方面。

1) 命名

文件命名约定是最有用的内容管理技巧之一。例如，可以使用字母、数字、代码来表示数字媒体类型、流派、艺术家和序号等。如果能够坚持使用一套设计完善的文件命名标准，则可以有效地管理任意数量的文件。

2) 文件夹和服务

通过将数字媒体文件分别保存在单独的文件夹中，可以根据自己的标准来汇集内容。请尽量减少文件夹的数量以避免混淆和冗余。

3) 档案

要保持数字媒体库的时效性，不仅需要增加新的可用内容，还需要将旧的或过时的内容存档。通常删除不再使用的内容既不实际也不必要，但是应该将不再使用的内容从当前数字媒体库中删除，并适当存储以便日后检索。如果有必要，请使用文件压缩技术减小文件大小以便管理。

4) 备份和安全

内容库和其他所有数据存储库一样，容易遭受发本地网络的破坏或盗窃。

3. 实况内容

与播放预先录制的内容相比，播放实况内容具有明显的优势。一般来说，娱乐和新闻信息如果是实况广播，则其影响力更大，而某些即时信息如果是预先录制后才播放的，则可能对用户而言毫无价值。

制作实况广播内容不难而且花费也并不高。如果使用的设备适当，则即便是实况视频在播放时也相对容易。而且实况流可能只需要将编码器与电视台或广播电台的实况信号输入连接起来即可。

不管在什么情况下，将实况流式节目的准确时间和 URL 告知观众都是非常重要的。请尽早并经常地通知用户，确保他们知道连接到什么位置及何时进行连接。

对于任何复杂的项目，计划都是首要任务。因为通常无法修改或调整已经开始播放的实况数字媒体流，所以必须在节目开始之前对广播进行规划。

8.6.2 创建播放列表

播放列表就是自动播放媒体内容的列表，它可以使客户端自动循环或随机播放，省去了经常打开媒体文件的麻烦，在长时间欣赏媒体时非常实用。

1. 播放列表语法

播放列表基于可扩展标记语言（XML）。使用 Windows Media 播放列表编辑器创建和编辑播放列表的优点之一是不需要了解 XML 代码。在将所有的项目添加到播放列表中后，播放列表编辑器会自动将播放列表转换为基于同步多媒体集成语言（SMIL）2.0 的 XML 文档。请记住，在保存文件之前，对播放列表所作的更改或添加不会生效。不过，假如熟悉 XML，则可以使用文本编辑器（如记事本）来创建或修改播放列表文件。

在使用播放列表编辑器或文本编辑器创建播放列表后，可以将其指定为发布点源。如果将播放列表作为点播发布点源，那么它将在客户端取得连接时开始播放。如果将播放列表作为广播发布点源，那么它将在发布点启动时开始播放。Serverside_Playlist.wsx 是一个相当简单的播放列表，却可以创建很长很复杂的播放列表，其中包含许多复杂的计时元素和行为元素。如果要使用文本编辑器来创建播放列表文件，请确保遵循以下原则。

包含子元素的元素定义在一组开始和结束标记内。标记的表示方法是在元素类型两侧加上尖括号（< >）。以下是 smil 元素开始标记的示例<smil>。结束标记则需要在元素类型前再加一个正斜杠（/），如</smil>。开始标记和结束标记之间的任何内容均用做针对该元素及其内部任何元素的“指令”。不包含子元素的元素可以没有结束标记，该元素包含在一对尖括号之间并以正斜杠（/）结尾，例如，<mediasrc="content_clip1.wmv"/>。

属性定义了对应于特定元素性质的“名称-值”对，每个元素都支持一组不同的属性。如果元素具有指定的属性，那么在 XML 代码中属性将显示在元素的后面。例如，在下面一行中：

```
<mediasrc="content_clip1.wmv"/>
```

media 是元素的类型，而为该元素指定的属性和值如下所示。

- noSkip: true
- role: advertisement
- src: C:\WMPub\WMRoot\advert1.asf

元素、属性及其值是区分大小写的，指定属性值时请确保使用了正确的大小写形式，否则播放时将无法识别。预定义属性值，如 begin、end、true 和 false，都应该用小写来指定。

2. 利用 XML 元素构建播放列表

播放列表文件包含 7 种基本的可扩展标记语言（XML）元素：smil、media、seq、switch、excl、priorityClass 和 clientData。元素可以包含有关自身的信息，或者用于控制一个或多个其他元素的行为。通过安排这些元素并设置相应的属性值，可以控制播放列表的播放并确定其表示结构。

播放列表元素的组织方式定义了播放列表的控制结构。例如，如果在文本编辑器中打开一个播放列表，就会注意到某些播放列表元素包含在其他播放列表元素中。包含其他播放列表元素的元素称为“父元素”。父元素控制其内部所有元素（称为“子元素”）的行为。

7 个基本 XML 播放列表元素中有 6 个充当父元素：smil、seq、excl、media、priorityClass 和 switch。seq 和 excl 元素充当时间容器，负责控制子元素的时间安排。priorityClass 和 switch 元素充当控制容器，负责控制子元素间的交互。

以下示例显示了包含在 seq 元素中的两个 media 元素。

```
<seq>
  <mediasrc="File3.wmv"/>
  <mediasrc="File4.wmv"/>
</seq>
```

seq 元素的作用是按顺序播放自身所包含的元素。因此在上面的示例中，File3.wmv 首先播放，其次是 File4.wmv。这种将元素包含在其他元素内部的排列方式称为“嵌套”。

在播放列表中，smil 元素是文档根，也就是说，该元素是播放列表中所有其他元素的父元素。在下面的示例中，seq 元素是 smil 元素的子元素。seq 元素包含 media 元素和 clientData 元素，后两者分别由 src 属性和 title 属性修饰。smil 元素前面的 wsx 元素用于标明播放列表所采用的服务器端同步多媒体集成语言（SMIL）语法的版本。

```
<?wsxversion="1.0"?>
<smil>
  <seq>
    <mediasrc="file1.wmv">
      <clientDatatitle="MyFile#1"/>
    </media>
    <mediasrc="file2.wmv">
      <clientDatatitle="MyFile#2"/>
    </media>
    <mediasrc="file3.wmv">
      <clientDatatitle="MyFile#3"/>
    </media>
```



```
<mediasrc = "File4.wmv"/>
  <clientDatatitle = "MyFile#4"/>
</media>
</seq>
</smil>
```

在了解播放列表元素及其属性后，就可以构建很多有创意的解决方案来显示数字媒体内容了。

3. 使用 Windows Media 播放列表编辑器创建播放列表

除了可以自己利用 XML 标记元素创建播放列表外，还可以使用图形化的方式来创建，这更符合一般人的操作习惯，更加实用。

(1) 单击“发布点”项的“摘要”标签或者特定发布点的“源”标签界底部的“查看播放列表编辑器”按钮，打开 Windows Media 播放列表编辑器，如图 8-68 所示。

(2) 在工具栏上，单击“添加元素”按钮，打开如图 8-69 所示的对话框。在这里可以向播放列表中添加 media 元素。它的选择方法与源的选择方法一样，单击鼠标右键，在弹出的快捷菜单中选择【添加媒体】命令即可。添加的元素可以是单个媒体文件，也可以是目录。



图 8-68 “新建播放列表”窗口



图 8-69 “添加媒体元素”对话框

(3) 选择好后单击【添加】按钮把当前所选的媒体添加文件或目录到播放列表中。然后可在“内容的位置”文本框中重新指定新的要添加的媒体元素，直到所有的内容都已添加到播放列表为止。

(4) 单击【确定】按钮返回到如图 8-68 所示窗口。再在工具栏上单击“保存播放列表”按钮，打开如图 8-70 所示的对话框。在其中指定播放列表文件的名称和位置。播放列表文件必须使用.wsx 文件扩展名。最后单击【保存】按钮即完成新列表的创建。

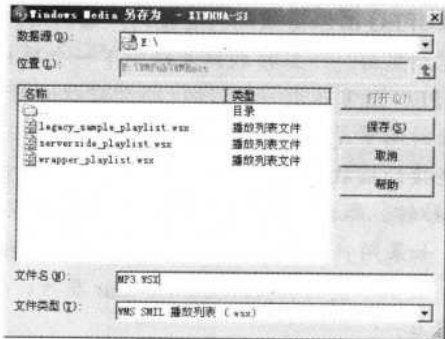


图 8-70 保存列表对话框

新添加的列表会在相应发布点“源”标签的媒体列表中出现，如图 8-71 所示。这样客户端在播放相应发布点的媒体文件时，就会自动播放包括新添加的列表中的媒体文件。

播放列表创建之后，可以供任何发布点使用。要将播放列表用于某个发布点，请单击该发布点“源”标签上的【更改】按钮（参见图 8-71 所示），把相应内容源指定到包括新建播放列表所在位置即可。



图 8-71 在发布点的媒体列表中的新播放列表



注意

Windows Media 播放列表编辑器仅在 Windows Media Services 管理单元中可用。由 Windows Media Services 传输的内容必须满足播放机所支持的最小内容长度以确保可靠地进行播放。Windows Media Player 9 系列支持的最小内容长度为 5 秒钟。Windows Media Player 早期版本支持的最小内容长度为 30 秒钟。如果要将播放列表文件保存到其他计算机或网络驱动器上，必须首先将共享权限授予 Windows Media 服务器。如果没有授予 Windows Media 服务器相应权限，则该服务器无法将文件写入远程网络驱动器。

如果播放列表中包括 JPEG 图像文件，则请不要将任何在播放机呈现图像时导致图像暂停的语法包含在播放列表中。用这种方式暂停 JPEG 图像可能导致播放机进入永久等待状态。如果一定要在这样的环境下显示静止的图像，则请创建该图像的视频文件，然后在播放列表中使用该视频文件。

如果播放列表中包括 JPEG 图像文件，并且该播放列表用于广播发布点，

那么请注意在 JPEG 图像播放期间连接到广播的用户将不会接收到该图像。相反，他们将看到黑屏。一旦播放列表转到下一个项目，播放将继续正常进行。如果希望让 JPEG 图像显示一段时间，那么应当使用 repeatCount 属性使该图像按较短的持续时间重复播放，以便达到预期的总体时间要求。这样，在图像播放期间取得连接的播放机就可以在图像重复时接收它了。例如，假设 JPEG 图像要显示 60 秒钟，那么可以设置 dur 属性值为 5 秒钟，且 repeatCount 属性值为 12。这样，如果用户在广播开始两秒钟后取得连接，那么再过 3 秒钟后图像将显示出来。假如不使用 repeatCount 和 dur 属性，那么在 58 秒钟的时间内用户只能看到黑屏。

8.6.3 使用 Windows Media 播放列表编辑器创建包装播放列表

包装播放列表是一种特殊类型的播放列表，可以使用它在发布点实施跟片广告。包装播放列表能够将内容附加到单播流的开头和末尾。

图 8-72 所示显示的是从服务器请求电影的客户端及客户端将随请求的电影一起接收的包装播放列表内容。

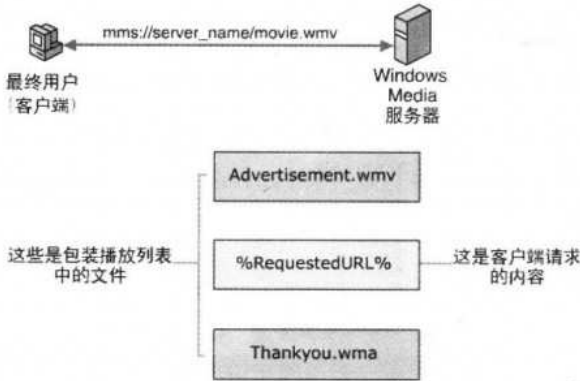


图 8-72 客户端请求和接收包装列表的流程

首先，客户端尝试连接到服务器。当服务器收到连接请求时，将查找与指定的 URL 相对应的发布点。在图 8-72 所示中，由于未指定发布点名称，因此该内容将连接到默认发布点。当包装播放列表能够用于发布点时，发布点同时传输在包装中指定的内容和用户请求的内容。发布点在传输请求的内容 (Movie.wmv) 之前传输 Advertisement.wmv，然后在该内容结束时传输 Thankyou.wma。

所有的发布点可指向同一个包装，这意味着只需修改一个包装播放列表文件即可应用通用的更改。对于可在一个包装中引用的流的数量没有限制，对于指向该包装的发布点的数量也没有限制。

可方便地使用包装播放列表自定义具有自己的商标和消息的流，而不必从内容制作者那里更改内容。另外，包装播放列表有助于确保连接到广播发布点的用户无论何时连接到广播，总是接收某些内容，如赞助商标识、免责声明或广告等。

包装是从发布点上的“广告”标签进行管理的，如图 8-73 所示。从中可以更改将哪些包装用于发布点、启用或禁用包装播放列表或者启动“创建包装向导”。



图 8-73 发布点“广告”标签

无论在哪种类型的发布点上启用包装，包装播放列表中包含的内容总是以点播内容的形式提供给用户。有关广告方面的内容，将在下节具体介绍。

使用 Windows Media 播放列表编辑器创建包装播放列表的方法如下。

- (1) 在 Windows Media 服务器控制台树中，单击要添加包装的发布点。
- (2) 单击“广告”标签（参见图 8-73 所示），然后单击界面底部的“包装编辑器”按钮，打开如图 8-74 所示的对话框。

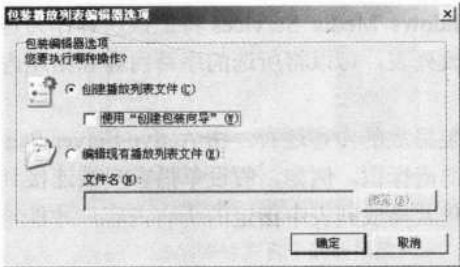


图 8-74 “包装播放列表编辑器选项”对话框

- (3) 选择“创建播放列表文件”单选项，然后清除“使用‘创建包装向导’”复选项的选择（也可以不清除，使用向导方式来创建）。

- (4) 单击【确定】按钮，打开如图 8-68 所示窗口。在工具栏上，单击“添加元素”按钮，同样会打开如图 8-69 所示的对话框。在这里指定要添加到包装播放列表的内容的名称和位置，向包装播放列表添加 media（媒体）元素。完成后，可以通过在播放列表树中拖动元素来安排播放顺序，如图 8-75 所示的就是添加，并调整了播放顺序后的播放列表。

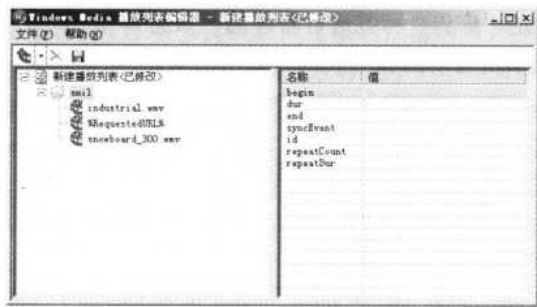


图 8-75 添加了播放列表后的“新建播放列表”窗口

(5) 在工具栏上，单击“保存播放列表”按钮，在打开的如图 8-71 所示的窗口中指定包装播放列表文件的名称和位置，包装播放列表文件必须使用.wsx 文件扩展名。这样就完成了包装播放列表的创建。

8.6.4 广告方案概述

使用流式媒体解决方案发布广告时，必须综合考虑要播放的内容类型、广告商的偏好，以及希望观众获得的观看体验等因素，调整好广告的优先级。为此，Windows Media Services 提供了大量广告选项。

1) 使用包装广告

当用户首次连接到服务器和内容流结束时，可以使用包装来提供广告或其他内容。在为内容指定一个包装时，Windows Media Services 将把该内容作为包装播放列表的一部分包含在其中。通过使用包装播放列表，可以将所选的序幕内容和结尾内容作为播放列表项目插入到主内容前后。

除广告外，常作为包装播放的内容还有：由 Active Server Page (ASP) 生成的动态播放列表、站点商标，以及赞助商标识。例如，假设单播客户端连接到已指定了包装广告的实况流，那么它只有在播放完包装播放列表中指定的所有内容后才能播放实况内容。

2) 显示插播式广告

可通过使用插播式广告将广告与播放列表中的其他内容混合在一起。播放列表中的广告可以来自本地服务器或广告服务供应商。

在实施插播式广告时，应考虑以下事项。

- 通过使用流切换在内容流之间进行切换。流切换可以对应于持续时间、脚本命令或客户端事件。
- 在播放列表中要显示广告的位置上使用指向特定广告服务供应商的 URL。通常，广告服务供应商会提供一个链接，该链接指向最符合用户概况的广告。
- 可以使用 noSkip 属性禁止用户跳过广告。
- 若要记录有关发布点的数据，并且需要区分广告和其他内容，请将广告内容的 role 属性值设置为 Advertisement。这样就可以在日志文件中搜索该值并选用相关的数据了。

3) 显示横幅广告

可以使用 Windows Media Services 在播放机中或网站上显示横幅广告。横幅可以包含任

意类型的数字媒体内容，如动画、视频流或音频流。例如，在通过服务器播放一首歌曲时，可以在横幅中显示有关艺术家、唱片集和音乐会日程的信息。或者可以在横幅中包含一个指向音乐会日程的链接，用户可以单击该链接转到音乐会促销商的网站，而不会干扰音频流。

在实施横幅广告时，应考虑以下事项。

- 横幅可以在整个播放列表持续时间内显示，也可以在播放内容流中的各个新片段时发生变化。
- 可通过引用动态 URL（通过读取来自广告服务供应商的 cookie 而创建）为每个用户显示自定义横幅。
- 基于播放持续时间来轮换显示横幅。
- 还可以使用横幅空间显示其他基于 Web 的信息，如新闻和广告链接。
- 设计各种大小的横幅，具体情况取决于广告商的要求和个人的需要。无论播放机如何实现（嵌入式播放机、标准播放机还是外观模式播放机），横幅广告都可以显示。

横幅的实现方法有两种：将广告横幅 URL 与公告文件中的 Banner 元数据元素相关联，或者使用服务器端播放列表中 clientData 元素的 bannerURL 属性。

4) 选择广告架构

Windows Media Services 支持在 Windows Media 服务器上安置广告内容及引用位于广告服务供应商处的广告内容。亲自安置广告时，由自己控制和存储广告内容。可以直接跟踪广告消费并应形势的变化修改内容。

如果与一个广告服务供应商签约，那么将由广告服务供应商控制和存储广告内容。可以在播放列表中包含对用于安置广告内容的服务器的引用。由广告服务供应商负责报告广告使用情况。

许多系统都使用亲自安置广告和从广告服务供应商处获取广告的组合形式。这种组合具有既可对相关广告进行本地控制又便于通过广告服务供应商带来更多收入的优点。

5) 创建广告策略

可以使用策略控制用户接收广告内容的方式。广告策略通过组合使用下列手段确定用户体验。

- 事件：可以使用事件触发某个广告的开关。例如，在实况广播流中，可以使用事件插入地区性广告以代替全国性广告，反之亦然。
- 播放列表属性：可以配置播放列表属性来控制用户的广告体验。例如，如果将 noSkip 属性设置为真，那么用户播放机上的快进和定位控件将被禁用。只有广告播放完成，用户才能继续接收播放列表中的内容。

8.6.5 在流中添加包装广告

在流中添加包装广告的步骤如下。

(1) 在控制台树中，单击要添加包装播放列表的发布点，然后选择“广告”标签，单击界面底部的“包装编辑器”按钮，打开如图 8-74 所示的“包装播放列表编辑器选项”对话框。

(2) 选择“创建播放列表文件”单选项，同时选择“使用创建包装向导”复选项，单

击【确定】按钮后打开如图 8-76 所示向导首页对话框。

(3) 单击【下一步】按钮，打开如图 8-77 所示的对话框。单击【添加广告】按钮，打开如图 8-78 所示的对话框，在这里要选择广告文件。

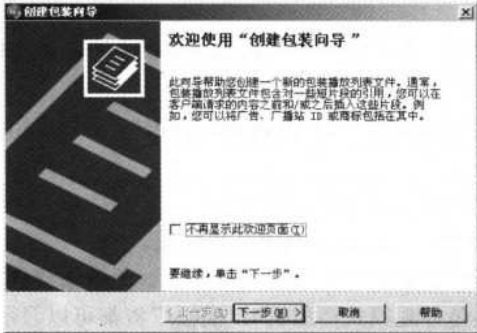


图 8-76 “欢迎使用‘创建包装向导’”对话框

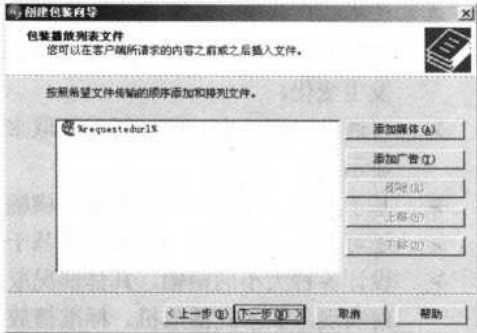


图 8-77 “包装播放列表文件”对话框

(4) 单击【确定】按钮返回到如图 8-77 所示的对话框中，单击【下一步】按钮，打开如图 8-79 所示的对话框。在这里要选择播放列表文件的保存位置，通常是某发布点的源位置。

(5) 单击【下一步】按钮，打开向导完成对话框。单击【完成】按钮即完成在流中添加广告的全部过程。

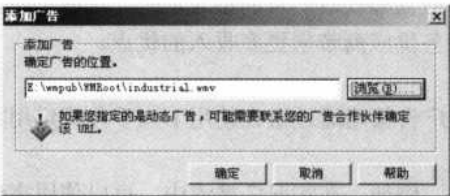


图 8-78 “添加广告”对话框

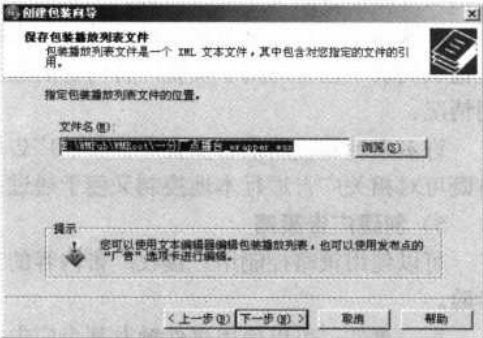


图 8-79 “保存包装播放列表文件”对话框

(6) 在如图 8-73 所示“广告”标签上，单击【更改】按钮。在打开的对话框“位置”文本框中键入包装播放列表文件的路径，或者单击【浏览】按钮以定位到文件。最后单击【确定】按钮返回到“广告”标签界面中，选择“将包装程序与此发布点一起使用”复选项，完成整个配置过程。

其他类型包装播放列表广告的添加过程都差不多，在此不再赘述。

8.7 Windows Media 编码器的使用

前面已介绍了 Windows Media 编码器的安装，本节要介绍这款软件在文件格式转换方面的应用，也就是将保存在硬盘或光盘上的多媒体文件转换为 Windows Media 服务可使用的流

媒体文件格式，这种文件格式的转换过程就称为“编码”。

Windows Media 编码器的功能完全可以从程序启动时自动（如果取消了“启动时显示此对话框”复选项的选择，则不会在启动时显示）打开的如图 8-80 和图 8-81 所示的两个对话框中体现。在图 8-80 所示中列出了四项主要功能：广播实况事件、捕获音频或视频、转换文件、捕获屏幕；而在图 8-81 所示的对话框中也列出了四项主要功能：捕获实况内容用于本地播放、捕获实况内容用于流、将胶片内容转换为视频、广播公司会议。



图 8-80 “向导”标签



图 8-81 “快速启动”标签

Windows Media 编码器 9 系列是一个功能强大的制作工具，用于将实况和预先录制的音频和视频转换为 Windows Media 文件或流。下面对图 8-80 所示的四项主要功能分别予以简单介绍。

8.7.1 广播实况事件

通过安装在计算机上的设备捕获音频或视频，然后对这些内容进行实况广播，广播方式有两种：通过推传递将流传输到运行 Windows Media Services 的服务器上，或者允许 Windows Media 服务器和播放机通过拉传递直接从编码器接收流。

（1）在如图 8-80 所示的对话框中双击“广播实况事件”选项，打开如图 8-82 所示的向导对话框。在这里要选择当前计算机上使用的音频、视频设备（因为笔者计算机上没有连接视频设备，所以呈灰色不可选状态），并且还可以单击相应选项后面的【配置】按钮对设备进行属性设置。

（2）单击【下一步】按钮，打开如图 8-83 所示的对话框。在这里要选择一种广播编码内容的方法。如果编码器位于防火墙后面，或者希望从编码器发起连接，那么通过推传递将流从编码器发送出去是很有用的，选择“推传递到 Windows Media 服务器”单选项。例如，假设你刚刚接到最新通知，公司总裁要向员工播发一个讲话，Windows Media 服务器位于公司防火墙之外的远程位置上，而此时正是服务器管理员午夜休息的时间。通过将流以推传递方式从编码器发送出去，可以使流穿过防火墙，既满足了总裁的要求，又不用打紧急电话叫人来管理服务器。

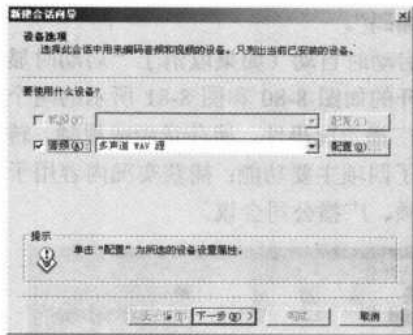


图 8-82 “设备选项”对话框

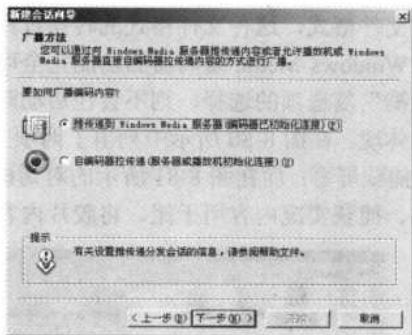


图 8-83 “广播方法”对话框

选择“自编码器拉传递”单选项，则允许 Windows Media 服务器通过拉传递接收流，这在许多方案中都是很有用的。首先，如果有多个分发服务器存在，并且各自在不同的时间进行连接，那么可以让各个服务器在做好准备播放准备时发起与编码器的连接。其次，如果要将服务器和编码器之间的带宽用量降至最低，那么可以从服务器中进行拉传递。例如，服务器管理员可以添加一个发布点，并将其配置为根据客户端请求自动启动，也就是说服务器直到第一个客户端取得连接时才发起与编码器的连接。这将消除服务器和编码器之间不必要的带宽占用。最后，如果服务器位于防火墙后面，那么从服务器进行拉传递也很有用。例如，假设你要在举行会议时播发事件，因而将编码器设置在了公用网络上。这时就需要将流传输到位于受保护网络中的某个分发服务器上。此时，服务器管理员可以用拉传递方式通过防火墙接收流。

当预计不会有很多客户端收看流时，允许播放机以拉传递方式接收流是很有用的。Windows Media 编码器最多允许 5 个客户端在广播过程中直接与其连接。当允许播放机以拉传递方式接收流时，可以通过 IP 地址或者 IP 地址组限制对内容的访问。

（3）如果选择的是“推传递到 Windows Media 服务器”单选项，单击【下一步】按钮，打开如图 8-84 所示的对话框。这时要设置 Windows Media 服务器和发布点信息。

如果在上一步选择的是“自编码器拉传递”单选项，则打开的是如图 8-85 所示的对话框。在这里要求选择编码器与服务器，或者播放机连接所用的 HTTP 端口，一般按默认设置即可。

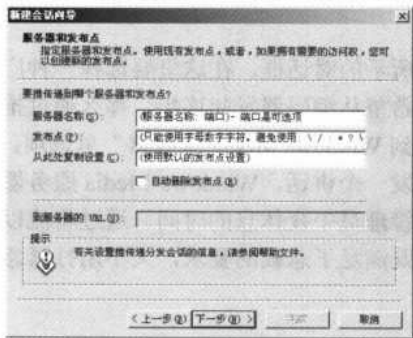
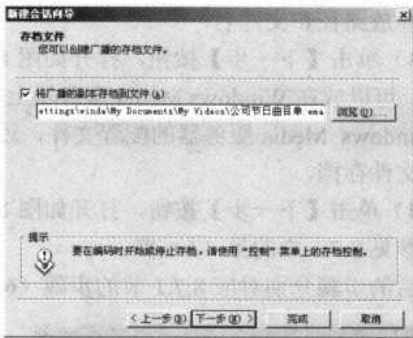
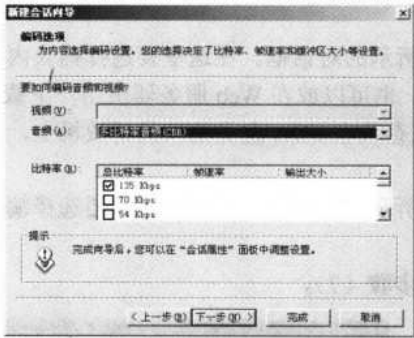


图 8-84 选择推方案后的“服务器和发布点”对话框 图 8-85 选择拉方案后的“广播连接”对话框

（4）无论是从图 8-84 所示还是从图 8-85 所示的对话框中单击【下一步】按钮，都可打开如图 8-86 所示的对话框。在这时要选择音频、视频比特率，比特率越高音质越好，或者画面越

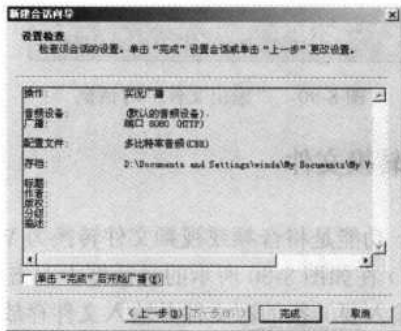
清晰，但所占用的带宽也越高，要充分考虑到用户所用的网络连接方式和用户数等因素。执行到这一步可以直接单击【完成】按钮结束向导，也可继续单击【下一步】按钮继续配置其他选项。

(5) 单击【下一步】按钮，都可打开如图 8-87 所示的对话框。在这里可以配置一个用来保存实况广播的副本文件，这有时很有用。



(6) 单击【下一步】按钮，可打开如图 8-88 所示的对话框。在这里可以配置广播实况内容的一些基本标题和版权信息，也可不用配置。

(7) 单击【下一步】按钮，打开如图 8-89 所示的对话框。这是一个向导完成对话框，在其中显示了以上各步设置的摘要。确认无误后单击【完成】按钮即可完成一个实况广播会话的创建。



如果在最后出现错误提示，不能创建成功，通常是由于 Windows Media 服务器上的 HTTP 协议没有启用。如果在 Windows Media 服务器上不能启用 HTTP 协议，则可能是由于 IIS 正在使用 HTTP 协议所需的 80 号端口，可以更改 Windows Media 服务器上 HTTP 协议所用端口，也可停止 IIS 的运行。通常不采用更改 HTTP 协议端口。

8.7.2 捕获音频或视频

这一功能是通过安装在计算机上的设备捕获音频或视频，然后将捕获的内容转换为

Windows Media 文件，以便日后进行分发。

(1) 在如图 8-80 所示的对话框中双击“捕获音频或视频”选项，打开如图 8-82 所示的对话框。在这里也是选择捕获设备。

(2) 单击【下一步】按钮，打开如图 8-90 所示的对话框。在这里要指定捕获内容保存的文件存放路径和文件名。

(3) 单击【下一步】按钮，打开如图 8-91 所示的对话框。在这里要选择捕获内容分发的方式。可以放在 Windows Media 服务器上分发，也可以放在 Web 服务器供用户下载，或者当做 Windows Media 服务器的配置文件，还可以存放在 PDA 之类的口袋播放机上，也可以仅作为文件存档。

(4) 单击【下一步】按钮，打开如图 8-86 所示的对话框。在这里也是要选择编码的比特率，参见 8.7.1 中的第(4)步。

随后的步骤分别对应 8.7.1 节的步骤(6)和步骤(7)。



图 8-90 “输出文件”对话框

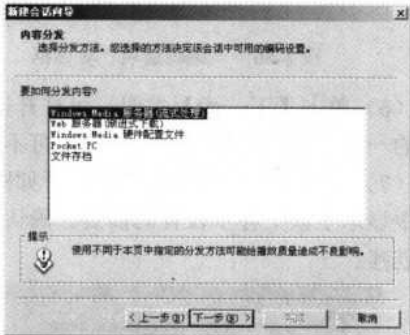


图 8-91 “内容分发”对话框

8.7.3 转换文件

这一功能是将音频或视频文件转换为 Windows Media 支持的格式，以便日后进行分发。

(1) 在如图 8-80 所示的对话框中双击“转换文件”选项，打开如图 8-92 所示的对话框。在这里输入要转换的源文件并输入文件存放路径和文件名。

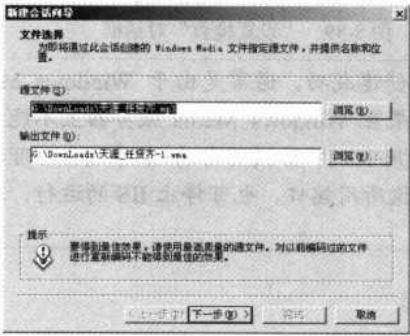


图 8-92 “文件选择”对话框



图 8-93 “内容分发”对话框

(2) 单击【下一步】按钮，打开如图 8-93 所示的对话框。在这里要选择一种内容分发方式。在此以选择“文件下载”方式为例进行介绍。

(3) 单击【下一步】按钮，打开如图 8-94 所示的对话框。在这里要选择编码所用的音频、视频设备和比特率。

随后的步骤分别对应 8.7.1 节中的步骤 (6) 和步骤 (7)。单击【完成】按钮即开始转换，转换后显示如图 8-95 所示的结果。

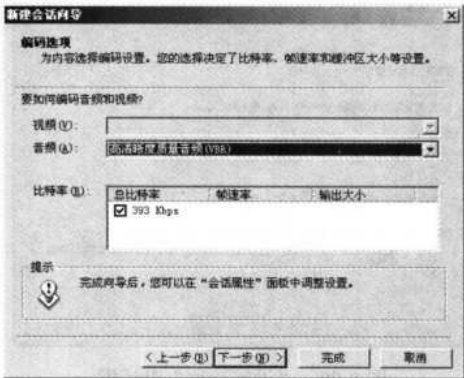


图 8-94 “编码选项”对话框

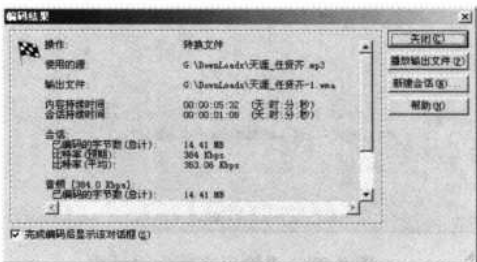


图 8-95 转换后的结果

8.7.4 捕获屏幕

这一功能是用来捕获当前计算机屏幕上的图像，包括鼠标指针的移动，可以捕获整个屏幕、屏幕的一个区域或者特定的窗口。

(1) 在如图 8-80 所示的对话框中双击“捕获屏幕”选项，打开如图 8-96 所示的对话框。在这里要选择捕获的窗口区域。

(2) 单击【下一步】按钮，打开如图 8-97 所示的对话框。在这里要选择具体捕获的端窗口。在“窗口”下拉列表中显示了当前计算机上所有已打开的窗口，如果选择了“捕获期间闪烁边界”复选项，则捕获的窗口在播放时会显示边界。

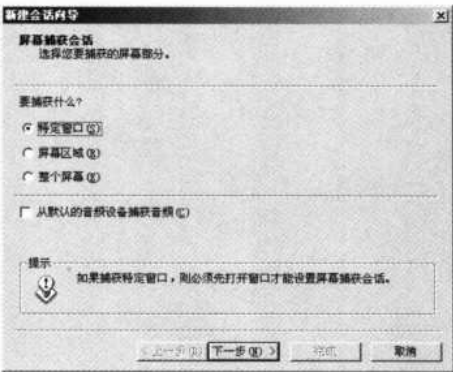


图 8-96 “屏幕捕获会话”对话框

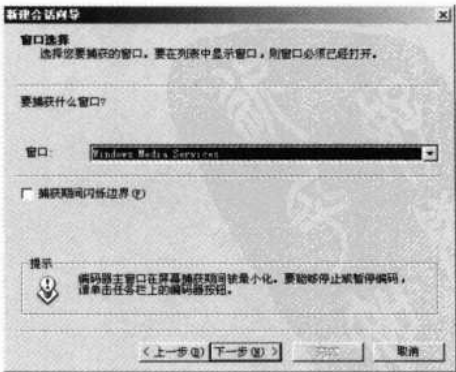


图 8-97 “窗口选择”对话框

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（3）单击【下一步】按钮，打开如图 8-98 所示的对话框。在这里要指定捕获窗口内容所输入的文件存放路径和文件名。

（4）单击【下一步】按钮，打开如图 8-99 所示的对话框。在这里要选择捕获窗口时编码的比特率级别，根据对视频质量的实际需求和客户端播放所用的网络连接方式，以及文件大小等因素而定。

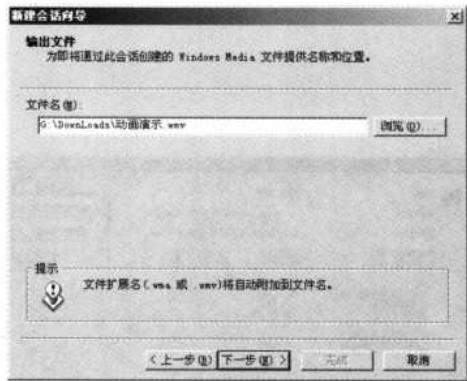


图 8-98 “输出文件”对话框

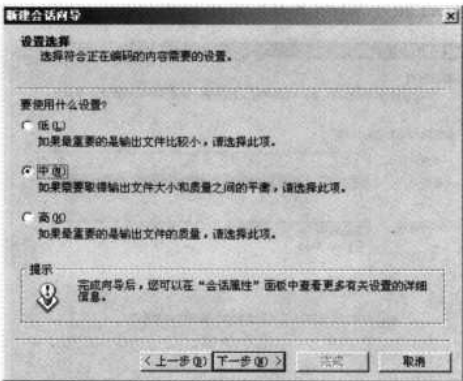


图 8-99 “设置选项”对话框

随后的步骤分别对应 8.7.1 节中的步骤（6）和步骤（7）。

有关编码器的使用就介绍这么多，因篇幅因素，其他有关基本属性配置在此就不一一进行介绍了。

第9章 企业 SharePoint 门户网站配置

目前，Microsoft SharePoint 的应用也是企业网络应用的一个热点，因为它可以将企业中的各种信息化软件系统，如 Office System 和 IIS 网站高度集成，将企业信息化提高到了一个新的高度。其实这也就是以前一直在倡导的企业信息化 MIS 平台。现在有了 Microsoft SharePoint 产品，实现起来就非常容易了。

在 Microsoft 的 SharePoint 产品家族中包括两款软件，那就是 SharePoint Services（目前最新版本为 3.0，但本章仍以主流应用的 2.0 版本进行介绍）和 SharePoint Portal Server（目前最新版本为 2007，但本章仍以主流应用的 2003 版本进行介绍）。通过综合这两者的协作功能，公司可以允许用户创建、管理和轻松构建自己的 SharePoint 站点和门户网站，并使得整个公司内部都能通过对门户网站的访问实现公司信息化平台访问的统一入口点。

SharePoint 产品和技术的设计目标是增强与 Microsoft Office System 的集成，允许创建团队和会议站点，并能够在 Office 应用程序内直接进行实时文档的协作。新的设计使得公司能够通过高级的用户配置文件功能，个性化定制他们的内部网和外部网门户体验，从而在一个统一的门户视图中通过 SharePoint 站点与内部和外部的团队成员开展协作，并能够通过容易配置的 Web 部件集成和访问业务链应用程序。

本章要通过一个示例介绍 Windows SharePoint Services 2.0 和 Windows SharePoint Portal Server 2003 在企业门户网站架设方面的应用。

本章重点

- Windows SharePoint Services 和 Windows SharePoint Portal Server 的关系
- Windows SharePoint Services 和 Windows SharePoint Portal Server 安装注意事项
- Windows SharePoint Services 网站创建与基本配置
- Windows SharePoint Portal Server 门户网站的创建与基本配置
- Windows SharePoint Portal Server 个人网站的创建与配置
- Windows SharePoint Portal Server 门户网站的基本管理

9.1 Windows SharePoint Services 和 SharePoint Portal Server

Microsoft SharePoint 产品和技术实现了公司内部轻松、相互联系的协作。通过综合 Microsoft Windows SharePoint Services 2.0 和 SharePoint Portal Server 2003 的协作功能，公司可以允许用户创建、管理和轻松构建自己的 SharePoint 站点，并使得整个公司内部都能访问这些站点。

9.1.1 Windows SharePoint Services 2.0

Windows SharePoint Services 是一个用来创建能够实现信息共享和文档协作的 Web 站点的引擎，也可以说是一种应用服务器，有助于提高个人和团队的生产力。它是 Windows Server 2003 中所提供的信息工作体系结构的重要组成部分，为 Microsoft Office System 和其他的桌面应用程序提供了附加的功能，并能够作为应用程序开发的平台。

Windows SharePoint Services 站点将文件存储带入了一个新的水平，为团队协作提供了一个活动空间，它使基于文档、任务和活动的协作成为可能，并且使得共享联系人和其他信息的过程变得更为轻松。Windows SharePoint Services 允许团队和站点的管理人员更容易地管理站点内容和用户活动。该环境旨在更为轻松和灵活地部署、管理和应用程序开发过程。Windows SharePoint Services 2.0 允许团队出于信息共享和文档协作的目的创建 Web 站点，从而有助于提升员工个人和团队的生产力。

1. SharePoint Services 网站的主要功能

基于 Windows SharePoint Services 2.0 的网站为使工作组进行通信、共享文档和共同完成项目提供了场所，可以说是一个集成化的企业信息化平台，可以为工作组当前正在处理的每个项目创建一个单独的网站，仅使用一个 Web 浏览器就可以参与网站讨论。但是，如果使用与 Windows SharePoint Services 兼容的客户端程序（如 Microsoft Office 2003），就可以在工作时与网站无缝结合在一起，从而可以将文档保存到库中、在客户端程序中编辑文档及将信息移动或链接到网站。

可以在 SharePoint 网站添加信息，例如，事件、与工作组通信的人员的姓名和电话号码及待办项目，还可以执行下列操作：

- 发送文档以便与其他工作组成员共享。
- 举行新闻组风格的讨论。
- 通过工作组投票表决来制定决策。

当工作组成员添加或者删除文档、列表、讨论及调查时，Windows SharePoint Services 会自动更新指向内容的链接，以便让成员轻松找到这些内容。还可以创建通知，以便在网站发生更改时获得通知。网站中的网页显示信息列表，允许工作组成员按照任何希望的方法组织信息，比如按主题、截止日期或作者进行组织。例如，可以执行下列操作：

- 限制显示，使用户只能查看应用于该用户的信息集合。

- 隐藏自己不感兴趣的信息。
- 更改信息列出的顺序。
- 设置自定义视图，以使工作组成员迅速将注意力集中于有关信息。

2. Windows SharePoint Services 2.0 的主要改进

SharePoint 站点由 Web Part 和基于 Windows ASP.NET 的组件组成。Web Part 设计用来向站点中添加界面，它由站点管理员和用户进行配置，能够创建基于界面的完整应用程序。Windows SharePoint Services 在发售之时已经附带了众多易于使用的 Web Part；在将来，可以通过 Microsoft 及其他第三方厂商获得更多的 Web Part。在 2.0 版本中，主要改进体现在以下几个方面。

1) 团队社区

SharePoint 2.0 站点为员工交流文档、思想、信息及沟通提供了一个场所。团队成员可以通过这些站点方便地加入到讨论之中，围绕共享文档展开协作和调查。站点内容可以通过 Web 浏览器和支持 Web 服务的客户端工具加以访问。文档协作特性允许用户轻松签入、签出文档，并对文档实施版本控制。

2) 提高员工能力

SharePoint 站点成员可以查找重要的联系人和专家，并与之进行沟通和交流，而且这一切既可以通过电子邮件也可以通过即时消息来完成。站点内容可以被轻松搜索，用户还可以接收到通知信息，告知现有文档和信息已经进行了修改，或者有新的信息或文档被添加到站点之中。站点内容和布局可以针对用户的个人喜好加以个性化定制，还可以使用 Web Part 就某个主题向特定用户展示有针对性的信息。

Microsoft Office 程序可以使用 SharePoint 站点的内容。站点上的所有协作内容，例如，文档、列表、活动、任务分配及成员名册等，都可以在 Microsoft Office Word 2003、Microsoft Office Excel 2003 和 Microsoft Office PowerPoint 2003 中读取，还可以对 Web 图片库中的图片进行编辑。Microsoft Office Outlook 2003 允许同时查看 SharePoint 站点的活动日程和个人日程，它还可以创建特定于某个会议的工作区，以便讨论会议的具体召开时间和地点。

3) 管理功能

SharePoint 站点的管理人员可以定制站点内容和布局，以确保站点成员可以访问和利用重要的相关站点信息。如果需要，管理员还可以对成员的参与行为进行监视。安全性和工作职责不仅是灵活的，而且是易于访问的。经过精心设计的列表和整个站点可以保存为模板并被整个组织范围内的员工个人、团队或企业部门重复使用。

4) 管理和部署

Windows SharePoint Services 可以进行伸缩，以容纳组织内部的数以千计的站点。它完全支持负载均衡的 Web 场和群集数据库部署。对于站点和服务器的管理人员来说，他们不仅可以对存储设定和应用配额，而且可以对每个服务器上的站点和每个站点中的用户设定并应用配额。站点的使用情况能够被监视，以检查并清除不再使用的站点。安全选项不仅数量详尽而且易于管理。服务器的管理人员可以委派最终用户创建他们自己的站点。他们还可以通过 Web 浏览器、命令行工具或者可以访问 Web 服务的对象模型对站点和服务器加以管理。

5) 集成化的 Windows .NET 部署

除了 Web Part 基础结构之外，Windows SharePoint Services 的服务器、站点及站点内容

546 网管员必读——网络应用（第2版）

都可以通过一个完善的、基于 Windows .NET 的对象模型和符合行业标准的 Web 服务暴露给外界。也可以使用 Microsoft Office FrontPage 2003 对站点进行定制并增强由数据驱动的站点内容。

9.1.2 SharePoint Portal Server 2003

SharePoint Portal Server 2003 是一个可伸缩的门户服务器，连接到整个业务流程中的所有个人、团队和知识。它提供了一个具有以下功能和特性的安全企业商务解决方案。

- 通过单点登录和企业应用程序集成功能，将来自不同系统的信息集成到一个解决方案中。
- 提供灵活的部署和管理工具。
- 实现了个人、团队和信息的整合、组织及搜索，简化了端到端的协作。
- 通过门户站点的内容和布局的定制和个性化，以及目标受众功能，使用户能够快速找到相关信息。

Microsoft Office SharePoint Portal Server 2003 将业务流程中的人员、工作组和知识连接在一起。它将分散的信息统一起来，便于就文档、项目和其他工作进行协作，并根据用户的功能组和组织角色呈现特定应用程序和自定义内容。SharePoint Portal Server 可与 Microsoft Windows 资源管理器、Microsoft Office 应用程序和 Web 浏览器协同工作，帮助在整个组织范围内创建、管理和共享内容。借助于 Windows Server 2003、SharePoint Portal Server 与 Office 2003、Windows SharePoint Services 和 SQL Server 2000 SP3 集成在一起，创建将整个组织连接起来的统一门户网站。

1. SharePoint Portal Server 的基本功能

SharePoint Portal Server 可以提供以下方面的解决方案。

1) 企业集成

在企业集成方面，SharePoint Portal Server 可以提供以下三方面内容：

- 伸缩和管理最大型组织的门户网站。
- 将不同系统集成到一个解决方案中。
- 为多个来源创建索引、搜索多个来源并提供对密切相关的信息的访问权限。

2) 管理、组织和发布内容

在管理、组织和发布内容方面，SharePoint Portal Server 可以提供以下三方面内容：

- 提供多种方法来按照有意义的方式（如按区域或主题）组织内容，从而更便于用户查找和管理。
- 对内容发布更大的控制能力。例如，可以提供指向特定访问者的内容。

3) 连接协作

在连接协作方面，SharePoint Portal Server 可以提供以下三方面内容：

- 允许查找人员、工作组、网站、现有最佳实践方案等，并与人员和工作组协作或者使用网站和使用最佳实践方案。
- 提供基于 Web 的交互式工作组网站。
- 为整个组织提供文档协作。

4) 用户的个人环境

在用户的个人环境方面，SharePoint Portal Server 可以提供以下三方面内容：

- 提供一个场所，以记住用户的身份和工作。
- 使信息工作人员能够实现门户个性。
- 为网站管理员提供灵活的个性化策略。

2. SharePoint Portal Server 2003 的主要改进

SharePoint Portal Server 2003 是 SharePoint Portal Server 2001 的更新版，提供大量的改进功能。主要体现在以下几个方面。

1) 为网站用户设计的新功能

以下是几个为 SharePoint Portal Server 用户设计的新功能。

■ 区域。

使用区域可以在门户网站上组织信息。如果发现区域中缺少有用的列表，可添加列表，请求内容管理者批准。可以在门户网站的多个区域中添加列表。

■ 新闻。

SharePoint Portal Server 使你能够通过新闻区域中添加列表，突出显示如公告和其他主要公司信息等信息。新闻列表可以是基于文本的内容，也可以是指向现有新闻项目（例如，新闻稿或新闻服务中的文章）的链接。

■ 个人网站。

“我的网站”是提供个性化和自定义信息的个人 SharePoint 网站。另外，“我的网站”还使你能够快速访问到完成工作所需的内容，例如，指向文档、人员或网站的链接，以及跟踪对门户网站和组织内的内容所做更改的通知。从“我的网站”中，还可以更新用户配置文件，以及与其他门户网站用户共享链接。

■ 用户配置文件。

可用于方便地查找有关人员及其文档和共享链接的信息。

■ 通知。

立即获得以电子邮件发送的通知结果，或者获得有关门户网站内容的每日或每周摘要。现在除了可以为新闻、区域、主题、搜索查询、文档和向后兼容文档库添加通知以外，还可以为人员、列表、列表项和网站目录添加通知。通知结果以易读的 HTML 格式显示，并且可以识别是否要因为更改或添加内容而发送通知结果。可以从“我的通知”界面管理所有通知。

■ 列表和视图。

由于 SharePoint Portal Server 是建立在 Microsoft Windows SharePoint Services 基础上的，因此可以在所有的 SharePoint 网站上添加预先设计好和自定义的列表。例如，可以创建一个图片库，来共享数字图片的集合，或者创建一个问题跟踪列表以维护有关特定问题的历史记录，还可以使用日历视图显示包含日期和时间列的任何 SharePoint 列表。此外，还可以在列表项中添加附件，包括 HTML 界面、文档和图像。

■ 简单的网站创建和界面自定义。

如果具有必要的权限，则可以通过使用“自助式网站创建”，根据要求创建 SharePoint 网站（例如，工作组网站或会议工作区网站），而不必借助 IT 部门的帮助。此外，还可以通过更改或添加 Web 部件来自定义界面。门户网站上的每个列表和库都是 Web 部件，使用浏

548 网管员必读——网络应用（第2版）

览器可以很容易地进行自定义和个性化操作。

■ 搜索。

较快的结果查询和提高的关联性级别使可以很容易地找到所需的信息。搜索结果包括人员、图片库、列表项和用户配置文件。如果搜索图像，则将看到图像的缩略图。如果搜索人员，则将看到此人（他或她）的个人配置文件。还可以按照不同方式（例如，按照作者、网站、日期或区域）对搜索结果进行分组。在搜索结果界面，可以将有用的搜索保存到我的链接 Web 部件。

■ 网站目录。

网站目录提供了一个中央位置，从该位置可以查看和访问与特定门户网站相关联的所有网站，还可以创建基于 Windows SharePoint Services 的网站或添加指向现有网站的链接。此外，向网站目录中添加网站是将内容包含于搜索结果的快速和方便的方法。

2) 为内容管理者设计的新功能

以下是为内容管理者设计的几个新功能。

■ 列表和视图。

同样，因为 SharePoint Portal Server 是建立在 Microsoft Windows SharePoint Services 基础上的，所以可以向所有 SharePoint 网站添加预先设计好的和自定义的列表。列表管理员可以批准或拒绝提交到列表的项目并添加注释。列表管理员还可以对列表应用权限，仅允许特定用户对列表进行更改。

■ 支持列表和网站模板。

用户可以将 SharePoint 列表另存为模板，并且可以重新使用它们或将它们分布到其他网站。可以将网站另存为模板以便捕获最佳方法或定义一致的外观。

■ 区域。

门户网站是内容丰富的子网站的层次结构，通过该层次结构，内容管理者可以向一个或多个区域中添加列表、图像和文档。内容管理者可以批准或拒绝提交到区域的项目。另外，在区域层可以对安全性进行管理，从而只允许特定用户对区域进行添加或更改。

■ 门户网站映射。

通过在 Web 浏览器的门户网站映射中拖动门户网站区域或主题从而对它们进行管理。可以使用门户网站映射创建、移动、重命名和删除区域。

■ 主题助手。

门户网站中的“主题助手”可以为区域推荐列表。内容管理者可以批准或拒绝这些建议。因为区域可以添加到门户网站，并且列表可以添加到区域，所以“主题助手”将持续了解和为每个区域推荐列表。

■ 网站目录。

要以有意义的方式组织和显示网站，可以创建对网站进行排序、筛选和分组的视图。网站目录还提供用来显示“最新网站”、“已添加网站”和“聚焦网站”的 Web 部件。网站目录可以配置为自动批准对网站的搜索，或要求对每个网站进行审批。

■ 新闻。

为了更加容易地管理新闻列表，可以指定内容显示的开始日期和结束日期，并自动隐藏过期的新闻项目。作为内容管理者，可以通过修改 Web 部件的属性来改变新闻列表的外观；

从标题行到摘要，再到扩展视图。

3) 为管理员设计的新功能

以下是对管理员有所帮助的新功能。

■ 体系结构。

- 可伸缩的分布式体系结构：SharePoint Portal Server 从单个服务器缩放至包含多个前端 Web 服务器和后端数据库服务器的服务器场。前端 Web 服务器无状态，因此可以平衡它们之间的负荷量，从而支持最大的组织。在使用共享服务拓扑结构时，最多可以在每个服务器场上部署一百个门户网站。
- 共享服务：将共享服务传送到中心管理和配置服务器场的多个门户网站中。共享服务可以包括创建索引和搜索、用户配置文件、访问群体、通知及个人网站。
- 使用 Extranet 与外界合作者进行通信：如果与外界合作者合作，或需要访问组织防火墙以外的数据，可以在 Intranet/Extranet 环境中使用 SharePoint Portal Server。在此配置下，内部和外部用户都将查看到相同的内容和数据并与之进行交互。另外，还可以使用防病毒保护和阻止的文件扩展名功能来保护服务器完整性。

■ 国际。

- 支持多语言网站：多语言网站可以驻留在单个服务器或运行 SharePoint Portal Server 的服务器场上。请注意，网站语言是独立于服务器语言的。
- 每个网站的区域设置：每个网站都可以有其自己的区域设置，如时间区。
- 新增分词：在此版本中不仅可以使用 SharePoint Portal Server 2001 中针对英语、法语、西班牙语、日语、泰语、韩语、繁体中文和简体中文的分词，而且还可以使用针对捷克语、芬兰语、匈牙利语和葡萄牙语的分词。

■ 管理。

- 通知：门户网站可以自动识别和优化可能生成大量结果的通知；它可以停用生成过量结果的所有通知。管理员可以停用或删除任何用户的通知和通知结果。通过锁定电子邮件地址域（只可使用用户配置文件中的数据）可以避免电子邮件出错。另外，还可以使用 .xsl 文件自定义通知结果电子邮件的格式。
- Single Sign-On：使用 Single Sign-On 可以存储和映射账户凭据，以便基于门户的应用程序从企业应用程序中检索信息时，用户不必再次登录。
- 安全集成企业应用程序：与 Microsoft BizTalk Server 2002 紧密集成可以借助 Single Sign-On 实现丰富和安全的企业应用程序集成。Actional 连接器能够与 PeopleSoft、SAP 和 Siebel 集成。
- 全文搜索：门户网站提供可扩展的高性能索引创建和查询处理基础结构。使用多服务器拓扑结构，可以通过将索引管理服务器中的内容索引传播到多个专用搜索服务器从而对资源进行管理。通过创建 HTTPS 协议的索引，可以实现在 SSL 上的网站爬网。此外，Windows SharePoint Services 网站的协议处理程序使得门户网站可以爬网网页、文档库、列表和列表项中的信息。Ifilter 除了具备搜索 Office Word (.doc)、Microsoft Office Excel (.xls)、Microsoft Office PowerPoint (.ppt)、MIME、XML 和 HTML 格式的文件的现有功能以外，还能

550 网管员必读——网络应用（第2版）

够对由 Microsoft Office Publisher (.pub) 和 Microsoft Office Visio (.vsd) 创建的文件进行全文搜索。

- 访问群体：访问群体允许组织根据用户的工作或任务为用户指定内容。可以将 Web 部件、新闻、列表和列表项指向一个或多个特定访问群体。使用 Microsoft Active Directory 目录服务中的内容，可以很容易地在现有分布列表和安全组中创建访问群体。
 - 备份和恢复：改进的备份和恢复功能可以灵活地恢复网站。服务器场中的每个网站都可以分别备份和恢复。此功能还可用于在删除非活动网站之前将其归档。
 - 用户配置文件：通过导入 Active Directory 中的属性和用户数据可以很容易地创建用户配置文件。借助用户配置文件可以很容易地查找人员并使得内容管理者可以通过使用访问群体确定信息指向。向灵活的用户配置文件中添加属性后，可以由集成的应用程序所使用，另外还使得门户网站用户可以更加容易地找到人员。
 - 非活动网站管理：管理员会定期要求网站所有者确认他们的网站是否在使用中或是要将它们删除。如果向网站所有者发出多个通知后，没有收到任何回复，则管理员可以指定自动删除此网站。
- 安全性。
- 标准 Windows 验证和安全方法：可以在使用任何 IIS 6.0 验证方法的同时使用 SharePoint Portal Server，可以使用 Microsoft Windows 验证或 Microsoft SQL Server 验证连接至数据库，并将 SharePoint Portal Server 与 Active Directory 集成到一起。
 - SharePoint 管理员组：允许域组的成员执行中心管理任务，而无须授予他们对本地服务器计算机进行管理的管理员权限。
 - 通过 SharePoint 管理中心管理用户：使用“SharePoint 管理中心”界面可以在所有网站上添加或删除用户并分配网站所有者。
 - 域组支持：使用域组可以控制对网站的访问。
 - 阻止的文件扩展名：服务器管理员可以阻止上传特定的文件类型（例如，.mp3 或.exe 文件）。

9.1.3 SharePoint Portal Server 与 SharePoint Services 之间的关系

许多人在应用 Windows SharePoint Services 和 SharePoint Portal Server 时就对两者的功能搞不清楚，为什么需要两个软件来实现类似的功能？其实我们完全可以把这两款软件理解为一个服务器软件的两个不同部分（其实笔者倒真的想建议 Microsoft 公司不要把这两款软件分离开来，而统一命名为 SharePoint 软件，当然这样捆绑在一起也可能带来销售方面的不利），前者主要负责基础站点的配置与管理，而后者则是对这些基础站点的集成和功能扩展，从而实现企业门户网站的组建与管理。两者的关系从管理角度来看，就是一个由分散管理到集中管理的提升；而从服务器的角度来看，两者的关系就是前端与后端的关系。

Windows SharePoint Services 为团队协作和生产力提供了站点，并且实现了大量智能空间。

SharePoint Portal Server 是一个服务器系统，它可以将多个 Windows SharePoint Services 站点集成起来，组成企业门户网站，并将这些站点空间与个人、知识和业务流程连接起来，实现了智能化的企业信息化平台。可通过使用 SharePoint Services 站点为个人、信息和公司创建门户网站点，也就是说，SharePoint Portal Server 充分利用了 Windows SharePoint Services 服务。



“门户网站”四个字可以这么理解，就是企业所有网络功能的唯一入口点。如 Windows SharePoint Services 可以为不同项目、主题创建不同的 SharePoint 站点，而 SharePoint Portal Server 可以把多个 SharePoint 站点集成起来，以一个统一入口来访问这些 SharePoint 站点。

虽然这些站点是专门针对 SharePoint Portal Server 的，但他们使用了 Windows SharePoint Services 平台所提供的各种技术，例如，Web 部件和 SharePoint 文档库。这种集成显著减少了开发、培训和支持的时间及费用。

SharePoint Portal Server 2003 为 SharePoint 站点提供组织和管理工具，从而扩展了 Windows SharePoint Services 的功能。它的站点注册表提供了一种企业范围的整合、组织和发布 SharePoint 站点的方式。另外，SharePoint Portal Server 还使得用户可以将存储在 Windows SharePoint Services 站点上的信息和文档发布给整个公司。SharePoint Portal Server 2003 还为企业提供了完整的附加功能，用来在业务流程中连接个人、团队和知识。它通过灵活地部署选项和管理工具，将多种系统中的信息整合到一个解决方案中。它简化了端到端的协作，使得信息工作者能够查找和利用整个公司内的个人、信息和 SharePoint 站点。SharePoint Portal Server 2003 还通过目标受众、个性化和定制工具，提供个人的相关信息。



SharePoint Services 和 SharePoint Portal Server 两者之间并没有双向必然的联系。SharePoint Services 是 SharePoint Portal Server 的基础，SharePoint Portal Server 需要 SharePoint Services 的支持，但 SharePoint Services 完全可以不需要 SharePoint Portal Server，独立完成它的企业站点开发任务，但它一般仅适用于中小型企业。可以这么理解，SharePoint Portal Server 组建的企业门户网站是 SharePoint Services 站点的集成和功能扩展，并且可以支持大型的服务器场，更适合于大型企业；而 SharePoint Services 站点只是一个个独立的小型网站，当然它也可以对这些小站点进行集中管理，但各 SharePoint 站点间没有任何关联。其实企业门户网站的组建最基础的工作还是 SharePoint Services 站点的配置。

SharePoint 产品和技术提供了灵活的部署和管理工具、高度可伸缩的协作解决方案。SharePoint 产品和技术还将实现更高层次的价值，提供一个可访问的、友好部署的、高度可伸缩的平台，用于开发扩展的应用程序。

9.1.4 配置 SharePoint 门户网站的基本思路

对于比较复杂的应用，在具体部署前掌握其基本的部署和配置思路是非常必要的。在 SharePoint 企业门户网站应用方面，基本的部署和配置思路如下。

1) SharePoint Services 2.0 和 SharePoint Portal Server 2003 程序的安装

与其他网络应用一样，在门户网站配置之前需要安装 SharePoint Services 2.0 和 SharePoint

552 网管员必读——网络应用（第2版）

Portal Server 2003 这两款服务器程序（分别负责前端和后端的工作）。

这一步看似比较简单，实则隐藏了许多很难预见的问题（笔者认为应该不会出现这些问题，应是软件本身存在的 Bug，期望新版本的 SharePoint Services 3.0 和 SharePoint Portal Server 2007 在这方面有所改进），初学使用的很难一次成功。笔者在刚开始摸索时，就曾遇到许多问题，一个程序反复安装了几天都没有解决本章中将要介绍的各种问题，其实网上也有许多网友提出这类问题，但并没有见到有效的解决方案。

具体参见本章后面的 9.2 节。

2) 配置虚拟服务器

SharePoint 站点的基础就是在 IIS 中创建的一个个虚拟服务器。要让这些虚拟服务器与 SharePoint Services 关联起来，就必须对这些虚拟服务器进行扩展，然后再进行各项配置，如顶级网站的建立、网站各种数据库的配置、网管用户组的配置、网站的安全性配置等。虚拟服务器的配置是在 SharePoint Services 管理中心进行的。

具体参见本章后面的 9.3 节。

3) 配置 SharePoint 站点

配置好站点中的虚拟服务器后，接下来就要对具体的 SharePoint 站点进行配置了，其中就包括站点所选用的模板、添加各种共享文档库、列表（其中包括联系人、链接、事件、任务和通知五部分）、图片库、讨论板和调查项目等，这就是 SharePoint 站点的五大功能。主要起到文件资源共享、协同工作、Web 论坛和用户投票的作用，基本满足了企业中所有的最基础信息化需求。

具体参见本章后面的 9.4 节。

4) 配置 SharePoint Portal Server 服务器

在这一部分中，首先也是要选择一虚拟服务器来进行扩展，以它为基础创建企业门户网站，然后再集成企业中已有的 SharePoint 站点。配置各种扩展功能和门户网站属性，如网站结构、网站数据库、网站用户、网站所有者等。

具体参见本章后面的 9.5 节。

5) 企业门户网站的使用与管理

本步就介绍以 SharePoint Services 站点为基础，利用 SharePoint Portal Server 服务器程序组建的企业门户网站的基本使用方法与管理方法。

具体参见本章后面的 9.6 节。

9.2 程序安装及其注意事项

在本节所介绍的整个服务器程序安装过程中包括三大部分：其中之一就是 Windows SharePoint Services 2.0 的安装，另外还有 SharePoint Portal Server 2003 和 SQL 2000 桌面引擎程序的安装。要真正完全正确地安装并配置这款服务器程序并不是那么容易，总是会出现许多意想不到的问题。笔者曾经试过许多次，几乎每一次都不是那么顺利，绝不会像一般的 Windows 程序安装那么简单，而且还需要事先满足一定的安装条件。本节主要向大家介绍一些关键的安装步骤和特别需要注意的地方。

9.2.1 程序安装条件

Windows SharePoint Services 2.0 和 SharePoint Portal Server 2003 推荐安装在 Windows Server 2003 成员服务器中，而且两个程序必须安装在同一个服务器中，建议不要安装在域控制器中。在安装 Windows SharePoint Services 2.0 和 SharePoint Portal Server 2003 前需要检查当前服务器系统是否满足以下所列的操作系统、软件和硬件配置条件。

1. 操作系统要求

Windows SharePoint Services 2.0 和 SharePoint Portal Server 2003 两服务器程序所支持的操作系统均仅为安装了 SP1 以上补丁的 Windows Server 2003。

2. 服务器要求

安装 Windows SharePoint Services 2.0 和 SharePoint Portal Server 2003 有下列要求。

1) 硬件要求

Pentium III 或兼容、700MHz 或更高处理器的 PC 机；最小 512MB 内存；最小 575MB 可用硬盘空间。

2) 软件要求

服务器需要下列操作系统之一。

- Windows Server 2003 Standard Edition，以及最新的 Service pack（补丁）。
- Windows Server 2003 Enterprise Edition，以及最新的 Service pack。
- Windows Server 2003 Datacenter Edition，以及最新的 Service pack。
- Windows Server 2003 Web Edition，以及最新的 Service pack。



注意

在 Windows Server 2003 Web Edition 上运行 SharePoint Portal Server 2003 需要在另一台计算机上安装 Microsoft SQL Server 2000。

3) 数据库要求

在 SharePoint Portal Server 2003 中包含着 Microsoft SQL Server 2000 Desktop Engine (SQL 桌面引擎，MSDE 2000) 的版本。但 SharePoint Portal Server 2003 不仅支持 MSDE 2000，还支持下列独立数据库。

- SQL Server 2000 Standard Edition，以及最新的 Service pack。
- SQL Server 2000 Enterprise Edition，以及最新的 Service pack。



注意

在域控制器上安装 SharePoint Portal Server 2003 需要使用 SQL Server 2000 Standard Edition 或者 SQL Server 2000 Enterprise Edition，以及最新的 Service pack，而不能使用 SQL 桌面引擎。

4) 网络要求

安装有 SharePoint Portal Server 2003 的服务器必须是 Windows NT 4.0、Windows 2000，或者 Windows Server 2003 域中的成员服务器，并且安装、启用了 IIS 6.0 和 ASP.NET 服务。

3. 客户端要求

客户端需要下列操作系统之一。

554 网管员必读——网络应用（第2版）

- Windows 98 或 Windows 98 Second Edition。
- Windows NT 4.0，以及最新的 Service pack 。
- 任何版本的 Windows 2000，以及最新的 Service pack。
- Windows XP Professional，以及最新的 Service pack 。
- 任何版本的 Windows Server 2003，以及最新的 Service pack。



注意

用于协调员的计算机，如果使用向后兼容文档库，需要下列操作系统之一：
任何版本的 Windows 2000、Windows XP Professional 或任何版本的 Windows Server 2003。

访问门户网站需要下列浏览器之一。

- Internet Explorer 5.01，以及最新的 Service pack。
- Internet Explorer 5.5，以及最新的 Service pack。
- Internet Explorer 6.0，以及最新的 Service pack。
- Internet Explorer 5.2 for Mac OS X，以及最新的 Service pack。
- Netscape Navigator 6.2 或者更高版本。
- Netscape Navigator 6.2 for Mac。
- Netscape Navigator 6.2 for UNIX

管理门户网站和区域需要下列浏览器之一。

- Internet Explorer 5.5，以及最新的 Service pack。
- Internet Explorer 6.0，以及最新的 Service pack。

9.2.2 SharePoint Services 程序的安装

安装 Windows SharePoint Services 服务器程序有两种方法：一种方法是通过“配置你的服务器向导”进行的，另一种方法是通过“控制面板”中的“添加或删除程序”工具进行的。下面介绍具体的安装步骤。但前提是必须满足以上条件，并且安装、启用了 IIS 6.0 和 ASP.NET 服务。在“Windows 组件”对话框中确保没有选中“FrontPage 2002 Server Extensions”选项，而确保选中了“公用文件”和“Internet 信息服务管理器”选项。如果要安装向后兼容文档库的组件，请确保选中“SMTP Service”选项，并且在安装以下服务器程序之前要为企业配置一个邮件服务器，因为在网站配置中需要用到用户的电子邮件。邮件服务器可以是 POP3 简单邮件服务器系统，也可以是 Exchange Server 这样的大型邮件服务器系统，当然也可以是其他第三方邮件服务器系统。

1. “配置你的服务器向导”法

（1）执行【开始】→【管理工具】→【配置你的服务器向导】菜单操作，打开如图 9-1 所示的对话框。如果在成员服务器中没有见到“配置你的服务器向导”菜单项，则可在“控制面板”的“管理工具”项下寻找。

（2）单击【下一步】按钮，打开如图 9-2 所示的对话框。或者执行【开始】→【管理工具】→【管理你的服务器】菜单操作，在打开的如图 9-3 所示的窗口中单击【添加或删除角色】按钮，也可打开如图 9-2 所示的对话框。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-1 “欢迎使用 ‘配置你的服务器向导’” 对话框



图 9-2 “预备步骤” 对话框



图 9-3 “管理你的服务器” 窗口

(3) 在如图 9-2 所示的对话框中单击【下一步】按钮，打开如图 9-4 所示的对话框。在“服务器角色”对话框中选择“SharePoint Services”选项。

注意 建议直接采用 Windows Server 2003 系统最新版本中集成的 SharePoint Services，而不要采用其他网上下载的，否则最终还是要升级到最新版本 Windows Server 2003 系统中的程序版本。

(4) 单击【下一步】按钮，打开如图 9-5 所示的对话框。这是一个“选择总结”对话框。



图 9-4 “服务器角色” 对话框



图 9-5 “选择总结” 对话框

(5) 单击【下一步】按钮，SharePoint Services 2.0 服务器程序便自动开始安装和配置。

安装和配置完成后打开如图 9-6 所示的对话框，提示目前服务器已成为 SharePoint Services 服务器。并在打开的“管理你的服务器”窗口中显示新安装的 SharePoint Services 服务器角色选项，如图 9-7 所示。



图 9-6 “此服务器现在已成为 SharePoint Services 服务器”对话框



图 9-7 “管理你的服务器”窗口中的“SharePoint Services 服务器角色”选项

2. “添加或删除程序”法

SharePoint Services 服务器程序除了通过“配置你的服务器向导”管理工具进行安装外，还可以通过“控制面板”中的“添加或删除程序”工具进行。在此仅介绍 SharePoint Services 程序组件的位置，如图 9-8 所示。

在安装过程中要求选择所安装的 SharePoint 服务器类型（如图 9-9 所示），可以是单服务器类型，也可以是由多个服务器组成的服务器场。在此仅以单服务器为例进行介绍，选择“典型安装”单选项。此时的数据库会以 Microsoft SQL Server 2000 Desktop Engine 数据库引擎担当，而不用另外专门配置 SQL 2000 数据库系统。

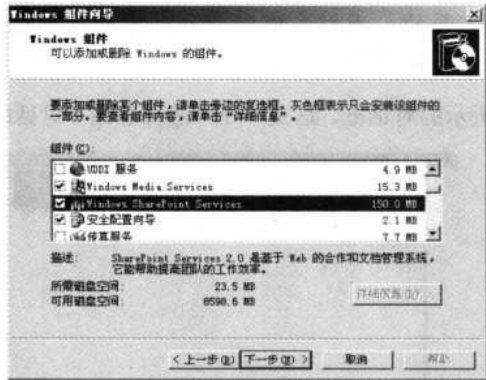


图 9-8 SharePoint Services 程序在“Windows 组件”对话框中的位置

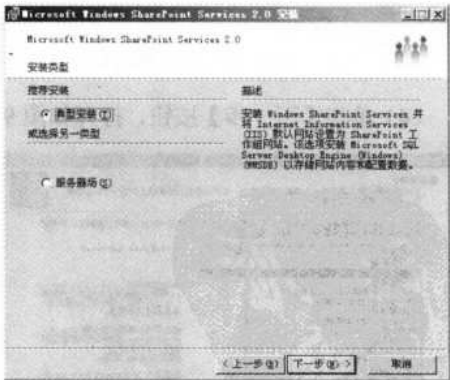


图 9-9 “安装类型”窗口



在以上两种安装方法中，程序均会自动安装 Microsoft SQL Server 2000 Desktop Engine 数据库引擎，因为 Microsoft SQL Server 2000 Desktop Engine 已包含在 SharePoint Services 程序包中。但如果 SharePoint Services 程序是在域控

制器中安装的，则后面附带安装的 SQL Server 2000 Desktop Engine 程序即使安装过程完全无误，也将无法正常工作，这一定要注意，否则可能安装了无数次，仍然发现 SQL 引擎程序不能正常工作。重新启动系统后，在系统状态栏中将显示 SQL Server 2000 Desktop Engine 引擎程序图标，但此时并不是正常工作的图标，如图 9-10 所示（空白的圆圈）。双击后再打开的窗口中也没有显示任何正在工作的 SQL 服务。如果是在符合以上条件的 Windows Server 2003 成员服务器上安装，则 SQL Server 2000 Desktop Engine 引擎程序图标应当如图 9-11 所示（圆圈中有一个绿色箭头）。而双击这个图标也会显示正在工作的 SQL 服务器和服务。

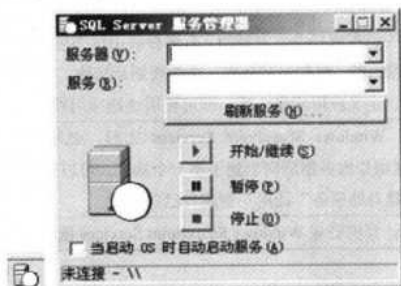


图 9-10 SQL 引擎程序工作不正常的图标和配置窗口



图 9-11 SQL 引擎程序工作正常的图标和配置窗口

在整个安装过程中需要进行一系列的 SQL 数据库引擎、SharePoint 网站和 Office 2003 程序配置。SharePoint Services 服务器程序正确安装后会打开如图 9-12 所示的 SharePoint 网站主界面（注意，其中的端口号不是固定的，每次安装都可能不一样）。如果没有出现这个网站主页，则证明程序安装不正确。



图 9-12 SharePoint 网站主界面

完成“配置你的服务器向导”，即完成了配置 Windows SharePoint Services 服务器，同时默认的网站也随 Windows SharePoint Services 一起进行了扩展，并可以立即使用，现可以为

组织配置 Windows SharePoint Services 和创建站点。表 9-1 列出了可在 Windows SharePoint Services 服务器上执行的一些其他任务。

表 9-1 可在 Windows SharePoint Services 服务器上执行的其他任务

任 务	任 务 目 的
配置默认电子邮件服务器设置	如果希望用户能够注册警报或获得加入站点的邀请，则必须连接到 SMTP 服务器和设置邮件要用到的电子邮件地址。这些设置也控制服务器发送的任何管理通知的电子邮件地址
安装与 Windows SharePoint Services 兼容的防病毒扫描程序，并启用防病毒扫描	通过安装和启用与 Windows SharePoint Services 兼容的防病毒扫描程序，帮助用户保护防止上传或下载带有病毒的文件
下载和安装可用的应用程序	通过下载和安装 Windows SharePoint Services 应用程序提高员工工作效率。这些应用程序是为满足特定的进程或任务而定制的。有多种应用程序可供选择，包括恢复、项目管理、技术支持问题跟踪、时间表和计划、事件规划及其他。安装或为进一步满足组织特定需求和要求而自定义应用程序之后，即可使用这些应用程序
创建其他站点或启用“站点创建自助服务”	用户在开始使用 Windows SharePoint Services 之前，必须有 Windows SharePoint Services 站点。扩展虚拟服务器后即创建了第一个站点。可以继续为用户创建站点，也可以打开“站点创建自助服务”让用户创建自己的站点
配置端口以允许远程管理	从网络中的其他计算机管理 Windows SharePoint Services 服务器

9.2.3 SharePoint Portal Server 2003 服务器的安装

注意 如果要组建企业门户网站，则需要安装 SharePoint Portal Server 2003 服务器程序，如果只要配置企业 SharePoint 信息化平台站点，则没必要安装。

SharePoint Portal Server 2003 服务器程序没有在 Windows Server 2003 系统中集成提供，需要另外购买。当然购买的 SharePoint Portal Server 2003 服务器程序其实也包括上节介绍的 SharePoint Services 和 Microsoft SQL Server 2000 Desktop Engine 数据库引擎程序，所以实际上可以通过这里的过程全面安装以上三大部分。这里介绍其基本的方法。

(1) 运行 SharePoint Portal Server 2003 服务器程序目录下的“setup.exe”，或者“Autorun.bat”程序，均可打开如图 9-13 所示的程序安装界面。



图 9-13 SharePoint Portal Server 2003 程序安装界面



注意

不要分别运行 SharePoint Services、Microsoft SQL Server 2000 Desktop Engine 和 SharePoint Portal Server 2003 程序文件夹下的“Setup.exe”文件来安装程序。另外，不支持在已经安装了 SharePoint Team Services 1.0 from Microsoft 的服务器上安装 SharePoint Portal Server 2003。在安装 SharePoint Portal Server 2003 之前，必须卸载 SharePoint Team Services。支持在装有 Windows SharePoint Services 的服务器上安装 SharePoint Portal Server 2003。

(2) 单击【安装 Microsoft Office SharePoint Portal Server 2003 组件】按钮，打开如图 9-14 所示的对话框。在其中列出了整个 SharePoint 服务器系统中所包括的三个程序部分：SharePoint Services、SharePortal Server 2003 和 Microsoft SQL Server 2000 Desktop Engine（此为可选项）。

(3) 单击【下一步】按钮，程序便自动开始安装。安装前，会有一个如图 9-15 所示的提示框，提示将暂时关闭 IIS、WWW、HTTP SSL 和 SMTP 服务。如果已通过上节介绍的方式安装了 SharePoint 组件，则会直接跳过图 9-14 所示的第一项 SharePoint Services 程序安装，立即进行后面两项程序的安装。否则会一一进行安装，进程如图 9-16 所示。



图 9-14 “安装 Microsoft Office SharePoint Portal Server 2003 组件”对话框



图 9-15 Microsoft Office SharePoint Portal Server 2003 组件程序安装提示框



图 9-16 程序安装进程

(4) 安装完 SharePoint Services 程序后打开如图 9-17 所示的窗口 Microsoft Office SharePoint Portal Server 2003 的安装。后面的几步分别像其他 Windows 程序一样，如选择接受许可协议、输入购买的许可密钥等。在此不再介绍。

随后的步骤中主要有两个地方要引起高度注意。其中之一是在安装过程中会要求用户输入一个 SQL 引擎程序安装选择和程序安装位置配置窗口，如图 9-18 所示。一般的中小型企业所采用的是 Microsoft Office SharePoint Portal Server 2003 自带的 SQL 2000 引擎，而不是采用专门的 SQL 2000 数据库系统，所以需要选择“安装（包含数据库引擎）”单选项。



图 9-17 “欢迎使用 Microsoft Office SharePoint Portal Server 2003 安装程序向导”窗口



图 9-18 “安装类型和文件位置”窗口

如果 Microsoft Office SharePoint Portal Server 2003 是在域控制器中安装的，则图 9-18 所示窗口默认选择“安装（不包含数据库引擎）”单选项，而且不可选，如图 9-19 所示，这是需要特别注意的地方。笔者曾经为此花费了好几天时间，总以为是系统配置问题。另一个特别要引起注意的地方是在安装过程需要指派一个用于配置、管理数据库的用户账户，如图 9-20 所示。

在这里输入时最容易犯的错误就是直接输入用户账户名和密码，但系统也不会提示错误。实际上这样输入是不行的，必须遵循以下基本输入格式原则：如果要采用域网络用户账户，则必须是“域\用户账户”的格式，如 grfw\administrator

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



注意

(grfw 为域名)；如果是采用本地成员服务器账户作为配置和管理数据库系统的用户账户，则应按“本地服务器计算机名\用户账户”的格式输入，如 grfwgz-s1\administrator (grfwgz-s1 为一成员服务器计算机名)，均不能直接输入用户账户名。如果是非域网络环境，则所指派的账户必须还是成员服务器本地的 Power Users 组成员。否则，在程序安装后，访问 SharePoint 时无论采取什么身份验证方式，也无论输入的用户账户和密码正确与否，均不能成功地访问网站，最终显示相应用户无权限。这是最容易出现的问题，笔者也为此付出了好几天的代价。



图 9-19 在域控制器中安装时的“安装类型和文件位置”窗口



图 9-20 指派配置与管理数据库的用户账户窗口

全部安装后的对话框如图 9-21 所示。安装完后系统同样需要花费较长时间进行各项配置。安装后也会打开一个 SharePoint Portal Server 2003 管理中心网页（如图 9-22 所示），如果网页显示正确，则证明程序安装、配置正确，可以开始使用了。最好是重新启动系统后再使用。



图 9-21 程序安装的进程对话框



图 9-22 SharePoint Portal Server 2003 管理中心网页

非常遗憾的是，即使到了最后，程序安装全部正常完成，进入 IIS 中，仍无法浏览 SharePoint 管理中心网站，如图 9-23 所示。有时还会显示“停止”状态，而且在执行启动命令时总是显示“参数不正确”，或者总是提示需要输入用户账户和密码，尽管用户账户和密码都是正确的，也配置了访问该网站的权限，仍是在不停地提示，根本无法进入网站，或者

直接显示如图 9-24 所示的错误提示。



图 9-23 IIS 中的 SharePoint 管理中心网站

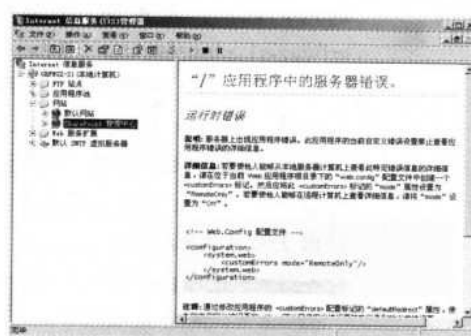


图 9-24 浏览 SharePoint 管理中心网站的错误提示

出现以上问题，除了可能是因为前面介绍的配置和管理数据库系统的用户账户指派时输入的用户账户格式不正确外，还可能是因为 IIS 中没有启用 ASP.NET。当然最主要的原因还是网站的“应用程序池”没有正确设置，或者根本没有正确安装。

在如图 9-25 所示的对话框的“应用程序池”下拉列表中可能显示的是“无效应用程序池”，或者其他选项，而不是“CentralAdminAppPool”，这样就会出现以上各种问题。出现这种现象时，你需要卸载 SharePoint Portal Server 2003 程序，重新启动系统后再安装。用前面介绍的格式指派数据库配置与管理账户，这样在程序安装后就会自动生成“CentralAdminAppPool”应用程序池了。

以上是单服务器、采用 SQL 2000 数据库引擎（仅支持 2GB 的数据库容量）情况下的程序安装过程及需要注意的事项，从中可以看出，在整个程序安装过程中充满了曲折，并不像想象中的那样简单。如果不采用 SQL 2000 引擎，而是独立安装 SQL 2000 服务器程序，安装方法一样，只是在如图 9-18 所示窗口中要选择“安装（不包含数据库引擎）”单选项，这样可以支持非常大的数据库容量，满足大中型企业的应用需求。下面再具体介绍两款服务器程序的基本配置和应用。



图 9-25 SharePoint 管理中心网站的应用程序池配置

9.3 SharePoint Services 虚拟服务器配置

要创建 SharePoint 站点，首先要对 IIS 中现有的虚拟服务器进行扩展，以实现与 SharePoint Services 关联。SharePoint Services 服务器的作用就是实现以网站的方式与其他 Web 网站、Office 办公系统和 SMTP 邮件系统协同工作，使用户可以仅通过 SharePoint 网站就可以实现绝大多数的日常办公应用。本节要介绍 SharePoint Services 虚拟服务器的主要配置方法。

9.3.1 SharePoint Services 站点基础

1. 关于网站和子网站

可使用顶级网站和子网站将网站内容划分为明确的、单独的可管理网站。顶级网站可以拥有多个子网站，而这些子网站自己也可以拥有多个子网站，可根据用户需要向下建设无限层次的子网站。由顶级网站和其所有子网站构成的整个结构称为网站集。

通过这种层次结构，用户可以有一个用于整个工作组的主工作网站，外加各个工作网站或用于从属项目的共享网站。顶级网站和子网站允许对网站功能和设置进行不同级别的控制。

2. 关于网站集管理员和“管理员”网站用户组

在 Windows SharePoint Services 中包括两级管理员：网站集管理员和作为“管理员”网站用户组成员的用户。网站集管理员对网站集中的所有网站具有所有权限。顶级“管理员”网站用户组的成员可以控制该顶级网站及任何子网站分支（从顶级网站继承权限）的设置和功能。例如，网站集管理员和顶级“管理员”网站用户组的成员都可以执行下列操作。

- 添加、删除或更改用户权限（如果已设置唯一权限）。
- 查看使用率统计信息。
- 更改区域设置。
- 管理 Web 部件和模板库。
- 管理 Web 讨论和通知。
- 更改网站的名称及说明、主题和主页组织形式。
- 配置顶级网站和所有子网站的相关设置，如区域设置。
- 更改顶级网站和所有子网站的可用权限。
- 更新顶级网站和所有子网站的电子邮件设置。
- 配置顶级网站和所有子网站的 Web 部件设置。

但是，当子网站使用单独的权限时，顶级“管理员”网站用户组的成员不能执行上面列出的操作。相比之下，网站集管理员可以在所有子网站中执行这些操作，无论子网站是否具有单独的权限。

子网站管理员用户组的成员只能控制该子网站及其所有子网站（继承上一级网站权限）的功能和设置。例如，子网站管理员可以执行以下操作。

- 添加、删除或更改用户权限（如果已设置唯一权限）。
- 查看使用率统计信息。
- 更改区域设置。

- 管理 Web 部件和模板库。
- 管理 Web 讨论和通知。
- 更改网站的名称及说明、主题和主页组织形式。

9.3.2 网站用户和权限

在进行具体的网站配置和使用，首先要清楚 SharePoint 网站中所定义的用户、组及其权限。

1. 关于网站用户组

Windows SharePoint Services 使用网站用户组来管理整个 SharePoint 网站的安全性。每个用户若要查看或访问 SharePoint 网站，则该用户至少应是某个网站用户组的成员。每个网站用户组都拥有相应的权限。权限是作为一个整体与系统相关联的规则，这些规则被授予本地组、全局组和用户。Windows SharePoint Services 中的权限可能是用户可以执行的操作，如“管理列表”。另外，还可以编辑分配到特定网站用户组的权限、创建其他网站用户组或者删除未使用的网站用户组。从 SharePoint 管理中心或者使用命令行管理工具，都可以管理 Windows SharePoint Services 中的网站用户组。



可以向 SharePoint 网站添加用户账户，而不用将他们分配到网站用户组。例如，可以创建用户账户，然后再将这些用户分配到网站用户组，还可以从所有网站用户组中删除用户。从所有网站用户组中删除用户时，该用户对网站将没有任何权限。

Windows SharePoint Services 默认包含下列网站用户组。

1) 来宾

具有有限的查看网页和特定网页元素的权限。此网站用户组用于给予用户访问特定网页或列表的权限，而不授予他们查看整个网站的权限。不能将用户显式地添加到“来宾”网站用户组中；如果用户以逐列表授予权限的方式获得列表或文档库的访问权，则该用户可以自动加入“来宾”网站用户组中。无法自定义或删除“来宾”网站用户组。

2) 读者

具有查看项目、查看网页和使用“自助式网站创建”功能创建顶级网站的权限。读者只能查看 SharePoint 网站的网页，不能添加内容。



“读者”网站用户组的成员使用“自助式网站创建”功能创建网站时，该用户将成为新网站的网站所有者和“管理员”网站用户组成员。这不会影响该用户对其他任何网站的网站用户组的成员身份。

3) 讨论参与者

具有“读者”权限，以及添加、编辑或删除项目，浏览目录，管理个人视图，添加、删除或更新个人 Web 部件和创建跨网站用户组的权限。“讨论参与者”网站用户组的成员无法创建列表或文档库，但他们可以向现有列表和文档库添加内容。

4) 网站设计者

具有“讨论参与者”权限，以及取消签出、管理列表、添加和自定义网页、定义和应用

主题和边框及应用样式表的权限。“网站设计者”网站用户组的成员可以修改网站的结构和创建列表、文档库。

5) 管理员

具有其他网站用户组的所有权限，以及管理网站用户组、管理列表权限，创建 SharePoint 网站、查看使用率分析数据的权限。无法自定义或删除“管理员”网站用户组。另外，在“管理员”网站用户组中，必须始终至少有一个成员。“管理员”网站用户组的成员对网站中的任何项目始终都有访问权，或者可以授予自己权限。



网站集的所有者和第二所有者是其网站的“管理员”网站用户组的成员，但在配置数据库中他们还被单独标识为网站集所有者。这个所有者标志只能通过使用 SharePoint 管理中心的“管理网站集所有者”页或者使用 Stsadm.exe 的 siteowner 操作进行更改。如果从网站的“管理员”网站用户组中删除所有者，则该所有者继续在数据库中保留所有者标志，并且仍然可以执行网站集管理任务。

这些网站用户组是按每个 SharePoint 网站进行定义的。分配到“管理员”网站用户组的用户只是某个特定 SharePoint 网站的管理员。若要执行任何会影响服务器计算机上所有 SharePoint 网站和虚拟服务器的管理性任务，用户必须是该服务器计算机的管理员（也称为本机管理员）或者 SharePoint 管理组成员，而不是某个特定 SharePoint 网站的“管理员”网站用户组的成员。

2. 自定义网站用户组的权限

可以创建网站用户组，或自定义现有网站用户组，以便让它只包括想要的权限（“来宾”和“管理员”网站用户组除外，它们不能自定义）。例如，为了只允许“网站设计者”编辑网站上的列表，可以从“讨论参与者”网站用户组中删除“编辑项目”权限。



某些权限依赖于其他权限。在编辑项目之前必须能够查看项目。如果某个权限从网站用户组中被删除，则任何依赖于该权限的权限也将被删除。例如，删除“查看项目”权限后，“添加项目”、“编辑项目”及“删除项目”权限也将被删除。同样，如果添加了需要其他权限的权限，所需的权限也将添加。所以，如果授予用户“编辑项目”的权限，“查看项目”权限将会自动授予。

3. 安全性和用户权限

用户权限授予用户对网站执行特定操作的能力，同时限制其他用户执行这些操作。某些权限不能完全限制特定的操作。“应用主题和边框”和“应用样式表”权限允许用户更改整个网站。但是任何拥有“添加和自定义网页”权限的用户都可以在实际的 HTML 代码中逐页地执行相同的更改。



如果授予用户“添加和自定义网页”的权限（通过将他们分配至包含此权限的网站用户组中），则同时授予了他们更改 SharePoint 中单个网页的主题、边框和样式表的能力。向网站用户组分配权限时，请确保分配了合适的权限，而不要无意中允许网站用户组的成员在 SharePoint 上执行的任务多于想要其执行的任务。相反，也要确保不会无意限制了网站用户组成员执行他们需要执行的操作。

4. 关于网站所有者和第二所有者

创建网站的用户会被列为该网站的所有者。根据配置的不同，可能还会要求该用户指定网站的第二联系人。如果有第二联系人的话，确认通知会自动发送给网站的所有者和第二联系人，具体配置将在本章后面具体介绍。

网站集的所有者和第二所有者是其网站的“管理员”网站用户组成员，但是他们还单独在配置数据库中标识为网站集所有者。这个所有者标志只能通过使用 SharePoint 管理中心的“管理网站集所有者”页或使用 Stsadm.exe 的 siteowner 操作进行更改。如果从网站的“管理员”网站用户组删除所有者，则该所有者继续在数据库中保留所有者标志，并且仍然可以执行网站集管理任务。

9.3.3 SharePoint Services 虚拟服务器扩展

SharePoint Services 服务器网站首先需要进行的的就是虚拟服务器扩展，就是把 SharePoint 服务与一个或多个虚拟的 Web 服务器关联起来，通过相应的 Web 服务器来实现网站内容的提供和管理。使用虚拟服务器扩展功能可在新的虚拟服务器上安装 Windows SharePoint Services、配置影响虚拟服务器上所有网站的设置或新建顶级网站。本节所介绍的虚拟服务器扩展的具体步骤如下。

(1) 在如图 9-12 所示管理中心主界面中单击“虚拟服务器配置”栏下的“扩展或升级虚拟服务器”选项，打开如图 9-26 所示界面。



图 9-26 “虚拟服务器列表”界面

(2) 在其中选择要扩展的虚拟服务器并单击。例如，此处以选择已有的“广州凌云计算机图书创作中心”虚拟网站服务器为例进行介绍。单击后打开如图 9-27 所示界面。



图 9-27 “扩展虚拟服务器”界面

(3) 单击“扩展并创建内容数据库”链接，打开如图 9-28 所示界面。这里有许多选项需要配置，如应用程序池、网站所有者的电子邮件账户和默认配额模板等。

配置好后单击界面下的【确定】按钮，系统便开始更新，最后显示如图 9-29 所示界面，显示虚拟服务器扩展成功。此时的所选网站已成为 SharePoint 门户网站的第一个顶级网站。再单击【确定】按钮，出现了一个专门用于扩展虚拟服务器设置的新界面，如图 9-30 所示。用以上同样的方法还可以把其他虚拟服务器扩展关联到 SharePoint 服务中，可以通过 SharePoint 管理中心管理多个 Web 服务器。

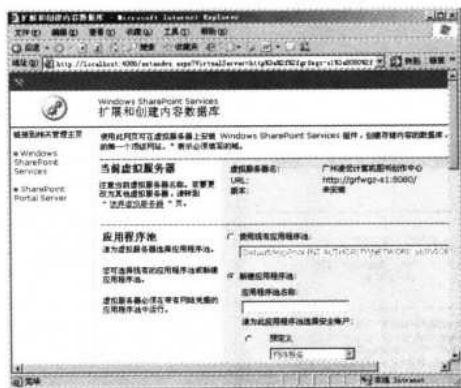


图 9-28 “扩展和创建内容数据库”界面

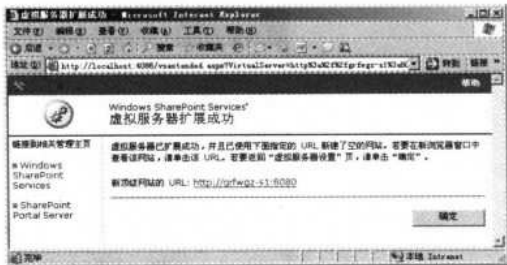


图 9-29 “虚拟服务器扩展成功”界面



图 9-30 “虚拟服务器设置”主界面



注意 注意扩展后的虚拟服务器将覆盖原有网站，这样原有网站的内容将不能访问了，所以，SharePoint 站点所用的虚拟服务器最好是以前为空白的站点。

9.3.4 扩展后的虚拟服务器配置

扩展虚拟服务器后，即可配置虚拟服务器的设置。本节所介绍的配置均是在如图 9-30 所示的虚拟服务器设置主界面中进行的。其中包括虚拟服务器配置、网站安全性配置、网站服务器连接配置和组件配置。下面仅对一些主要项目进行介绍。

1. 网站集自动化管理

使用这里所介绍的功能可允许用户组在此虚拟服务器上使用“自助式网站创建”创建自己的顶级网站。通过“使用确认和删除”功能可配置未使用网站集的自动删除。

(1) 在如图 9-30 所示主界面的“网站集自动化管理”栏下单击“配置‘自助式网站创建’”链接，打开如图 9-31 所示的界面。

“自助式网站创建”功能允许具有“使用自助式网站创建”权限的用户在指定的 URL 命名空间中创建网站。使用此网页可启用或禁用“自助式网站创建”功能。如果选择了“启用”单选项，并且要求“自助式网站创建”用户在登录页上提供第二联系人姓名，则还需要选择“需要第二联系人”复选项。

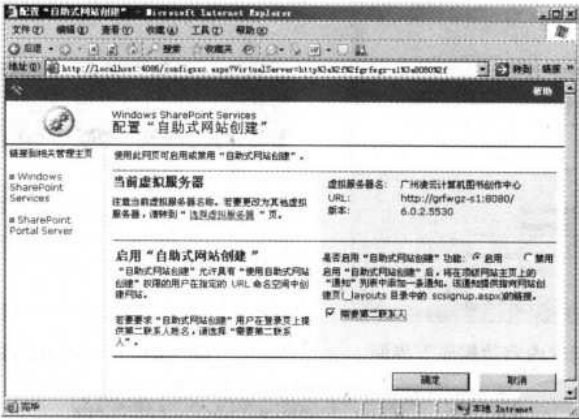


图 9-31 “配置-自助式网站创建”界面

设置好后单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。

(2) 继续在“网站集自动化管理”栏下单击“配置网站集使用确认和删除”链接，打开如图 9-32 所示的界面。使用此网页可要求网站所有者确认其网站集是否正在使用。另外，还可为未使用的网站集配置自动删除。

如果需要启用网站使用确认功能，则选择“向未使用网站集的所有者发送电子邮件通知”复选项，然后在下面的文本框中键入一个发送通知前已发现未使用的天数和邮件通知发送的频率。如果已启用通知，但并没有收到使用确认，则可选择“如果使用未被确认，则自动删除网站集”复选项，然后在下面的文本框中还可以指定是否在发送指定数量的确认通知后自

动删除该网站集。注意：自动删除会永久删除网站集和其下所有网站中的所有内容和信息。
设置好后单击【确定】按钮生效，并返回到如图 9-30 所示主界面。



图 9-32 “配置网站集使用确认和自动删除”界面

2. 安全性设置

使用这个栏目中的链接可按虚拟服务器的网站用户组建立权限。

(1) 在如图 9-30 所示主界面的“安全性设置”栏中单击“管理虚拟服务器的用户权限”链接，打开如图 9-33 所示的界面。其中包括：列表权限、网站权限和个人权限三部分。在这里可以指定网站用户组可具有的权限。使用这些复选框指定网站用户组拥有哪些权限。若要禁用权限，请清除权限名称旁的复选框。若要启用权限，请选中权限名称旁的复选框。使用“全选”复选框可选中或清除所有权限。



图 9-33 “管理虚拟服务器的用户权限”界面

配置好后单击【确定】按钮使设置生效，并返回到如图 9-29 所示主界面。

(2) 再在如图 9-30 所示主界面中的“安全性设置”栏中单击“管理 Web 部件页的安全性设置”链接，打开如图 9-34 所示设置界面。



图 9-34 “管理 Web 部件页的设置”界面

在这里要设置网站用户对“Web 部件连接”和“联机 Web 部件库”的访问权限。“Web 部件连接”权限用来指定是否允许用户通过将数据或者从源 Web 部件传递到目标 Web 部件来连接 Web 部件库；“联机 Web 部件”权限用来指定是否允许用户访问联机 Web 部件库。用户可以搜索、浏览和预览 Web 部件，并向 Web 部件页添加项目。如果你的服务器位于代理服务器或防火墙之后，你可能需要指定某些其他设置以启用联机 Web 部件库。

配置好后单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。

3. 虚拟服务器管理

使用这个栏目中的链接可创建或删除网站，配置虚拟服务器设置，如指定电子邮件服务器和数据库服务器，或指定配额、讨论设置、通知设置和版本控制的默认值。

(1) 在如图 9-30 所示界面的“虚拟服务器管理”栏中单击“虚拟服务器常规设置”链接，打开如图 9-35 所示的界面。



图 9-35 “虚拟服务器常规设置”界面

在“默认时区”区域中，选择用于虚拟服务器下的所有网站和子网站的时区，我国为“北京、香港特别行政区、乌鲁木齐”选项；在“默认配额模板”部分中，选择用做网站默认配额模板的配额模板。如果没有配额模板，则可以用“管理配额模板”页创建模板。注意，指定虚拟服务器的默认模板时，仍然可以在创建网站时选择其他模板。

在“人名智能标记和展示形式设置”区域中选中“启用成员的‘人名智能标记和联机状态’”下面的“是”或“否”单选项，以显示虚拟服务器下的所有网站的该信息。如果启用“人名智能标记和联机状态”，则当用户将鼠标指针悬停在此网站任何位置的成员名称上时，联机展示信息将显示在成员名称旁，并且人名智能标记也会显示。

在“最大上载大小”区域中键入允许的最大文件大小，默认值为 50MB。请指定单次上载到任何网站的最大允许大小。如果合计大小大于此设置值，则不会上载任何单个文件、文件组或内容。

在“通知”区域中指定通知的设置：

- 选择“启用”或“禁用”单选项，以允许或禁止此虚拟服务器下的所有网站的通知。
- 如果选择允许通知，并希望限制用户能够创建的通知数，请在“用户可创建的最多通知数”下输入一个值。若要使通知数目不受限制，可选择“不限制数量”，默认为 50 个。

在“网页安全验证”区域中，指定下列设置（在超过安全验证时间之后，用户将被要求重试其操作）：

- 选择“启用”或“禁用”单选项，以允许或禁止网页安全性验证。
- 若要设置到期时间，请选择“在此时间之后 ____ 分钟”，再键入安全性验证到期前等待的时间长度，或选择“从不”以使验证永不过期。

在“通过电子邮件发送用户名和密码”区域中指定是否通过电子邮件向用户发送其用户名和密码。如果关闭此选项，则只有在管理员更改新用户的密码并通知其新密码之后，该用户才可访问该网站。选择“是”或“否”单选项，以允许或禁止此选项。

在“启用了电子邮件的文档库”区域中指定是否允许文档库从公共文件夹中接收电子邮件附件。若选择“是”单选项，则请指定服务器名称和要使用的公共文件夹的根路径，并指定检查公共文件夹中的新电子邮件附件的频率。这只是对采用 Exchange Server 作为邮件服务器时才需要配置。具体设置如下：

- 选择“是”或“否”单选项，以允许或禁止电子邮件附件。
- 在“公共文件夹服务器和根路径”框中键入运行 Microsoft Exchange Server 的计算机的名称和该服务器上 Exchange Server 公共文件夹的根文件夹路径。
- 如果选择允许带电子邮件附件，请指定在公共文件夹中检查是否有电子邮件附件的频率和时间。

在“事件处理程序”区域中可以选择启用或禁用此虚拟服务器的事件处理程序。如果已禁用，则用户无法将文档库绑定到事件处理程序。选择“启用”或“禁用”单选项，以允许或禁止事件处理程序。启用此功能时，可以编写处理事件的代码，然后在文档库设置中指定特定文档库要使用的代码。

设置好后单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。

(2) 在如图 9-30 所示界面“虚拟服务器管理”栏中单击“管理内容数据库”链接，打开如图 9-36 所示界面。使用此网页可管理此虚拟服务器的内容数据库。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-36 “管理内容数据库”界面

在其中显示了当前虚拟服务器上已存在的内容数据库，如果要添加新的内容服务器（如进销存数据库系统、财务管理系统和 ERP 系统等），则单击“添加内容数据库”链接，打开如图 9-37 所示界面。在其中为新添加的内容数据库配置相关信息，如数据库名称、允许创建的网站最大数和警报数。



图 9-37 “添加内容数据库”界面

新添加了内容数据库后，单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。
(3) 在“虚拟服务器管理”栏中单击“虚拟服务器电子邮件设置”链接，打开如图 9-38 所示界面。在这里可以指定用于 Windows SharePoint Services 的通知、邀请和管理员通知的 SMTP 邮件服务器。可自定义“发件人地址”和“答复人地址”。



图 9-38 “虚拟服务器电子邮件设置”界面

配置好后单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(4) 再在“虚拟服务器管理”栏中单击“定义管理路径”链接，打开如图 9-39 所示界面。使用此网页可指定 URL 命名空间中由 Windows SharePoint Services 管理的路径（可对不需要的已有路径进行删除），还可添加子网站 URL。当然这都并非必须配置的选项。



图 9-39 “定义管理路径”界面



这时所说的“路径”并不是子网站，而是相当于网站文件夹的子目录。默认情况下，网站可以包括根目录和 sites 两级子目录，也可以创建其他的子目录。如要在网站上放置一个存放共享文件的文件夹，则还可以新建一个名为“share”（当然文件夹名称可以自定）的路径，然后把用于访问该网站用户共享的文件放到这个路径下即可。

配置好后单击【确定】按钮使设置生效，并返回到如图 9-30 所示主界面。

(5) 在“虚拟服务器管理”栏中单击“创建顶级网站”链接，打开如图 9-40 所示界面。使用此网页可新建顶级网站（如可以为各部门讨论分组，或者为具体项目等分别创建网站，这样便于管理，也对网站的安全性更加有利），当然这也不是必须配置的选项。



图 9-40 “创建顶级网站”界面

配置好后单击【确定】按钮使新建的顶级网站生效，并打开如图 9-41 所示界面，显示新添加的顶级网站地址。单击【确定】按钮返回到如图 9-30 所示主界面。如果需要添加多个顶

级网站，则按以上方法重复进行即可。

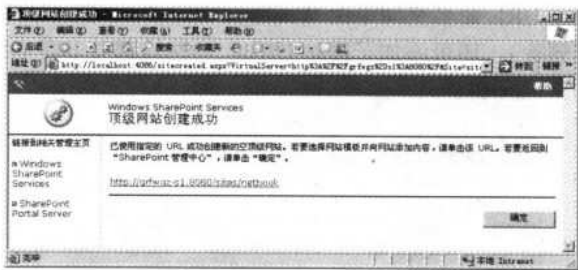


图 9-41 “顶级网站创建成功”提示界面

（6）在“虚拟服务器管理”栏中还有一项工作就是网站集的删除，直接在如图 9-30 所示界面的“虚拟服务器管理”栏中单击“删除网站集”链接，打开如图 9-42 所示界面。在其中的“要删除的网站的 URL”文本框中输入该虚拟服务器中已创建的网站地址。这主要是针对虚拟服务器中某些网站不需要时才执行。使用此网页上的设置可完全删除此虚拟服务器上的顶级网站及该网站的所有子网站。

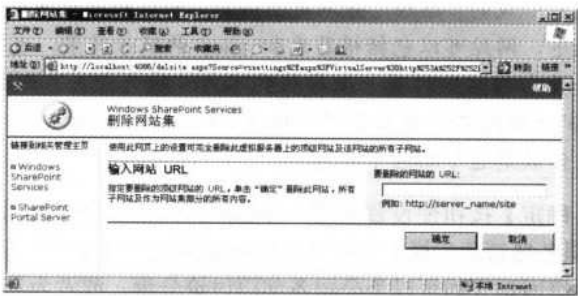


图 9-42 “删除网站集”界面

9.3.5 SharePoint 网站集安全配置

9.3.3 和 9.3.4 节中介绍的是针对具体的虚拟服务器进行的各项设置。一个 SharePoint 网站可以包括多个虚拟服务器，通过这里的设置就可以对各个虚拟服务器进行局部或全局设置。

（1）执行【开始】→【管理工具】→【SharePoint 管理中心】菜单操作，打开如图 9-12 所示主界面。

（2）在“安全性设置”栏中单击“设置 SharePoint 管理员组”链接，打开如图 9-43 所示界面。使用此网页可指定 Windows NT 安全组账户，以授予其 SharePoint 产品和技术的管理访问权限。组成员不一定非是执行 SharePoint 管理任务的本地管理员，本地管理员组的成员也可以执行 SharePoint 产品和技术的管理任务。



图 9-43 “设置 SharePoint 管理员组”界面

在“组账户名”文本框中输入 SharePoint 管理组，格式是“域/组账户”，当然如果不是域网络，也可以是本地组账户，格式为“成员服务器名/组账户”。此处笔者建了一个 SharePoint 组，专门负责 SharePoint 网站集的管理。

配置好后单击【确定】按钮使设置生效，并返回到如图 9-12 所示主界面。

(3) 在“安全性设置”栏中单击“管理网站集所有者”链接，打开如图 9-44 所示界面。使用此网页可查看和更改网站集的所有者和第二所有者。这些用户将收到所有有关配额和自动删除的通知，并具有网站集管理员权限。



图 9-44 “管理网站集所有者”界面

在“网站 URL”文本框中键入要管理网站集的完整 URL（如上节创建的各部门顶级网站），然后单击【查看】按钮以显示当前网站集所有者和第二所有者信息。在“网站集所有者信息”下的“用户名”文本框中输入网站集所有者用户账户，格式与前面介绍的一样。然后单击【检查名称】按钮以确认用户信息。用户成为网站所有者后，也会被添加到网站集管理员列表中。从网站所有者列表中删除用户也会将其从网站集管理员列表中删除，但不会更改已授予用户的任何其他组成员身份或权限。在“第二联系人信息”下的“用户名”文本框中键入该网站的第二联系人用户名，然后单击【检查名称】按钮以确认用户信息。第二用户可不配置。

配置好后单击【确定】按钮使设置生效，并返回到如图 9-12 所示主界面。然后以同样的方法为其他网站指定所有者用户名。

(4) 网站所有者全部配置好后，再在“安全性设置”栏中单击“管理网站用户”链接，

打开如图 9-45 所示界面。在此可以指定 SharePoint 网站的 URL，然后使用此网页查看和更改能够访问该网站的用户。

在“网站 URL”文本框中键入要管理的网站的完整 URL，然后单击【查看】按钮以检索此网站的网站用户组列表。若要添加新用户，请在“新用户账户信息”文本框中键入新用户信息，选择要包含该用户的网站用户组（可以是读者、讨论参与者、网站设计者和管理员四种类型之一），然后单击【添加用户】按钮添加相应用户。

如果要修改现有的用户账户，则可在“更改现有用户”栏中进行设置；若要编辑用户信息，则键入新信息，然后单击【更新】按钮；若要删除用户账户，则单击【删除用户】按钮。



图 9-45 “管理网站用户”界面

(5) 返回到如图 9-12 所示主界面，在“安全性设置”栏中单击“管理被禁止的文件类型”链接，打开如图 9-46 所示界面。使用此网页可禁止在此服务器上的任何网站上保存或获取特定的文件类型，以确保网站的安全。如果用户试图保存或获取被禁止的文件类型，则会收到错误消息，并且无法保存或获取该文件。只需在其中的下拉列表框中直接输入新的文件扩展名，添加文件类型即可。对于原来已添加的文件类型也可以进行编辑、删除。

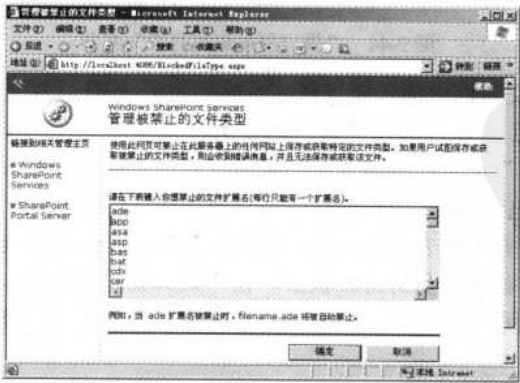


图 9-46 “管理被禁止的文件类型”界面

配置好要禁止的文件类型后单击【确定】按钮使设置生效，并返回到如图 9-12 所示主

界面。

(6) 在“安全性设置”栏中单击“配置防病毒设置”链接，打开如图 9-47 所示界面。使用此网页可配置病毒扫描的设置。你必须在承载文档的所有 Web 服务器上安装病毒扫描软件，这些设置才可生效。

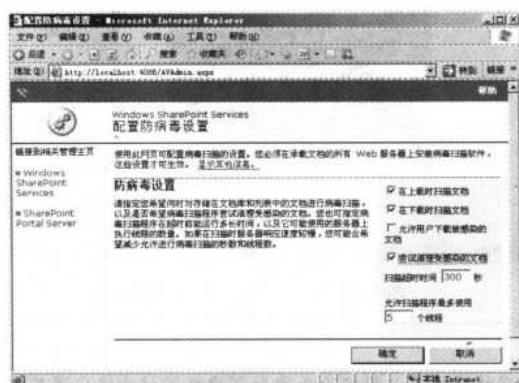


图 9-47 “配置防病毒设置”界面

可指定你希望何时对存储在文档库和列表中的文档进行病毒扫描，以及是否希望病毒扫描程序尝试清理受感染的文档。你也可指定病毒扫描程序在超时前能运行多长时间，以及它可能使用的服务器上执行线程的数量。如果在扫描时服务器响应速度较慢，你可能会希望减少允许进行病毒扫描的秒数和线程数。

9.4 SharePoint 网站的配置与使用

创建并配置好了 SharePoint 网站后，接下来就可以正式配置或使用 SharePoint 网站了。配置网站时须使用具有 SharePoint 网站管理权限的用户，而使用网站只需要有权限访问网站的用户即可。本节以管理员账户配置网站为例进行介绍，普通用户的网站使用方法与本节介绍的方法类似，只是有些功能普通用户不具有相关权限而已。有关网站用户、组及权限参见本章前面的 9.3.2。

9.4.1 网站模板的选择

虚拟服务器扩展后，首次以网站管理员的身份在浏览器中登录时就不会直接进入原来网站的主页了，而首先打开的是如图 9-48 所示界面。首先要求选择网站模板。

在 SharePoint 服务器程序中针对不同类型的网站用户提供了多种不同风格的功能集，适用于不同应用环境的网站模板。在如图 9-48 所示界面“模板”列表中进行了显示。每个模板都包含网页、Web 部件、列表、库和其他项目，根据实际需要选择与要创建的网站类型最接近的模板。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-48 “模板选择”界面



模板一旦被应用，必须删除或重新创建新网站才能应用其他模板。

“工作组网站”模板可用于工作组创建网站，以简便快捷地创建、管理和共享信息。该网站包括文档库和一些基本列表（如通知、事件、联系人和快速链接）。

“空白网站”模板可用于创建启用 Windows SharePoint Services 的带有空白主页的网站。可使用与 Windows SharePoint Services 兼容的网页编辑器添加交互式列表或任何其他 Windows SharePoint Services 功能。

“文档工作区”模板可创建用于工作组成员协同处理文档的网站。该网站可提供文档库（用于存储主要文档和支持文件）、任务列表（用于分配待办事项）和链接列表（用于存储与文档相关的资源）。

“基本会议工作区”模板提供了计划、组织和跟踪会议的所有基本要素。此会议工作区包含以下列表：目标、与会者、议程和文档库。

“空白会议工作区”模板是可根据要求进行自定义的空白会议工作区。

“决议会议工作区”模板是用于在其中查看相关文档和记录决议的会议工作区。此会议工作区包含以下列表：目标、与会者、议程、文档库、任务和决议。

“社会活动工作区”模板是用于社交场合的计划工具，提供有讨论板和可在其中张贴事件图片的图片库。此会议工作区包含以下列表和 Web 部件：与会者、交通指南、图像/徽标、携带物品、讨论和图片库。

“多页会议工作区”模板以多个界面计划、组织和跟踪会议的所有基本要素。此会议工作区包含以下列表：目标、与会者和议程，以及两个可根据需要进行自定义的空白页。

单击【确定】按钮后，如果选择的是“工作组网站”模板则打开如图 9-49 所示主页；如果选择的是“文档工作区”模板，则打开的是如图 9-50 所示主页。对比这两个网站主页就可以知道，网站的基本功能（在左边的导航栏中体现）都是一样的（在导航栏中都是列出了：文档、图片、列表、讨论和调查五大基本部分），只是一些子任务不一样而已，其他模板网站结构也基本一样，在此不一一介绍。



图 9-49 工作组网站模板的 SharePoint 网站主页

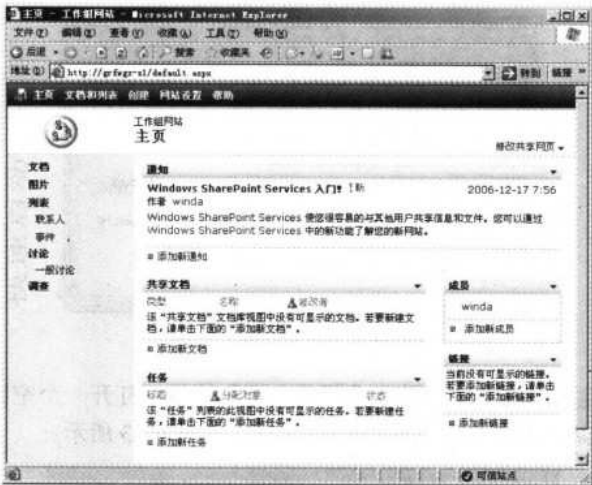


图 9-50 文档工作区模板的 SharePoint 网站主页

9.4.2 SharePoint 网站文档库配置与使用

在正式使用 SharePoint 网站各功能之前，必须进行相应的配置。如文档和图片共享，就必须先配置共享文件夹；要通过网站联系其他用户，则必须在网站中添加联系人；要与其他人共同讨论某个话题，则必须先创建讨论板等。这里首先介绍网站共享文档的配置。在此以在工作组模板中的如图 9-49 所示网站为例进行介绍。

1. 创建共享文档

(1) 在如图 9-49 所示网站中单击左边导航栏中的“文档”链接，打开如图 9-51 所示界面。

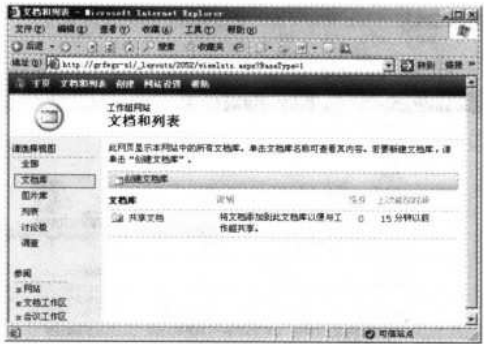


图 9-51 “文档和列表”界面

(2) 单击“共享文档”链接，打开如图 9-52 所示界面。在其中会显示当前所有已创建的共享文档（系统默认是没有任何共享文档的）。将文档添加到此文档库以便与工作组共享。



图 9-52 “共享文档”界面

(3) 如果要新建共享文档，则单击【新建文档】按钮，打开一个空白的 Word 文档，在其中编辑，编辑完成后在默认的保存位置进行保存，如图 9-53 所示。

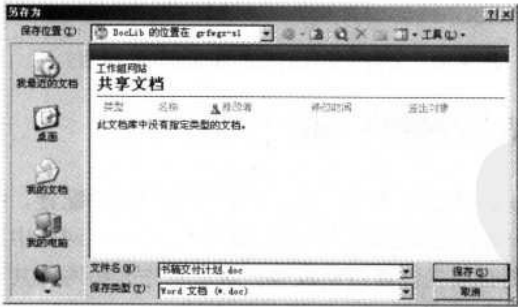


图 9-53 “另存为”对话框

如果要上传共享文件（不一定是 Word 文档），则在如图 9-52 所示界面中单击【上传文档】按钮，打开如图 9-54 所示界面，在其中输入要上传的文档路径，然后单击【保存并关闭】按钮即可完成单一文件上传。如果选择了“是否覆盖现有文件？”复选项，则如果文件名相同即覆盖原有同名文件。



图 9-54 “上传文档”界面

如果要上传多个文档，则在如图 9-53 所示界面中单击“上传多个文件”链接，打开如图 9-55 所示界面，在其中就可选择多个要上传的文件了。选择好后单击【保存并关闭】按钮退出并返回到如图 9-52 所示界面。



图 9-55 上传多个文件的界面

如果要为存放共享文件创建分类文件夹，则在如图 9-52 所示界面中单击【新建文件夹】按钮，打开如图 9-56 所示界面。在其中直接输入新文件夹的名称，然后单击【保存并关闭】按钮返回到如图 9-52 所示界面。此时会显示前面所新建的文档、上传的文件和新建的文件夹，如图 9-57 所示。

如果要查看网站中的共享文档列表，则可在如图 9-57 所示界面中单击【筛选】按钮，打开如图 9-58 所示界面。在其中就可以根据各种条件进行筛选查看。



图 9-56 “新建文件夹”界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-57 新建、上载文件和新建文件夹后的“共享文档”界面



图 9-58 “共享筛选”界面

2. “操作”行为配置

这里的设置其实是一个公共设置，适用于该用户对整个网站的访问。

(1) 在如图 9-58 所示界面左边导航栏中单击“操作”栏下的“通知我”链接，打开如图 9-59 所示界面。使用此网页可配置在此项目发生更改时创建电子邮件通知。配置好后单击【确定】按钮返回到如图 9-58 所示界面。

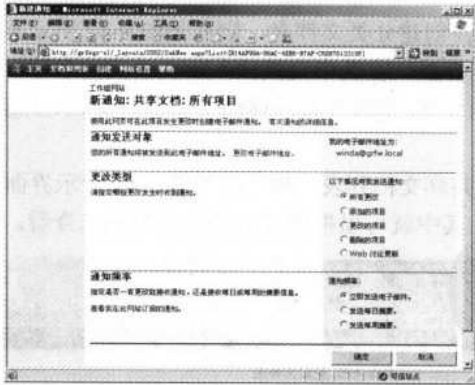


图 9-59 “新通知”界面

“通知”可将网站内容的任何更改通过电子邮件通知你。可以为列表和库以及其中各项创建通知。为列表或库创建通知时，可指定希望跟踪的更改类型。例如，可设置为在添加、修改或删除项目、文件时收到服务器通知，也可设置为在更新、删除文件或项目时收到文件和列表项目通知。对于库中文档，可设置为在添加、删除或编辑 Web 讨论中的评论时收到通知。可指定接收通知的频率，既可立即接收，也可接收每日或每周的摘要信息。如果不再需

要跟踪列表、库、项目或文件的更改，可在任意时间删除通知。



如果要从网站删除的用户创建通知，则必须手动删除他们建立的所有通知。对于将其安全性设置更改为有限访问的列表或库，此规则同样适用。如果用户为列表或库建立了通知，更改了安全性设置后他们将继续能够收到通知。一定要删除这些通知以阻止未经授权的用户拥有访问网站和用户信息的权限。

(2) 在如图 9-58 所示界面左边导航栏“操作”栏下面单击“导出到电子表格”链接，即可把当前网站上所有的文档列表以 Excel 文件的形式导出。

(3) 在如图 9-58 所示界面左边导航栏“操作”栏下面单击“修改设置和栏”链接，打开如图 9-60 所示界面。使用此网页可更改此文档库的设计，如名称、安全设置和栏。你也可创建或更改该文档库的视图。



图 9-60 “自定义共享文档”界面

(4) 单击“更改常规设置”链接，打开如图 9-61 所示界面。使用此网页可更改此文档库的常规设置。你可以更改名称、说明和其他设置，如是否将指向此文档库的链接显示在主页中的“快速启动”栏（也就是界面左边的导航栏，下同，不再赘述）上。为了网站美观起见，建议不要把太多的项目放在快速启动栏上。设置好后单击【确定】按钮使设置生效，并返回到如图 9-60 所示界面。

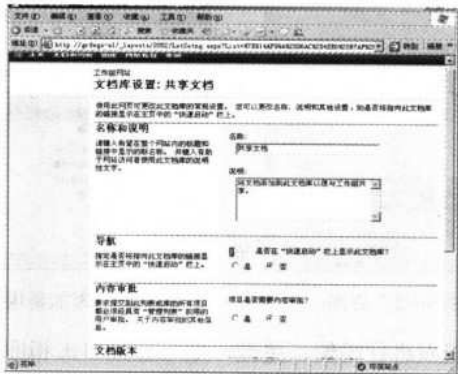


图 9-61 “文档库设置”界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(5) 在如图 9-60 所示界面中单击“更改此文档库的权限”链接，打开如图 9-62 所示界面。使用此网页可查看哪些用户能访问列表或文档库。如果要新建具有查看此文档库的用户，则单击【添加用户】按钮，打开如图 9-63 所示界面。在“步骤 1：选择用户”文本框中按“域\用户账户”，或者“成员服务器计算机名\用户账户”的格式输入新建的用户账户。这个账户必须是已存在域，或者当前成员服务器中已存在的。然后在下面的“步骤 2：选择权限”栏中为该用户分配访问该网站文档库的权限。

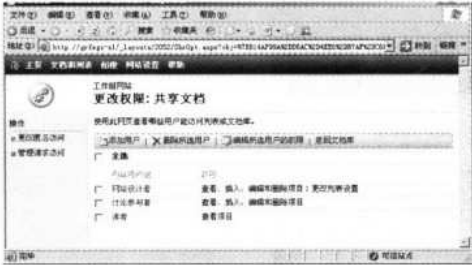


图 9-62 “更改权限”界面

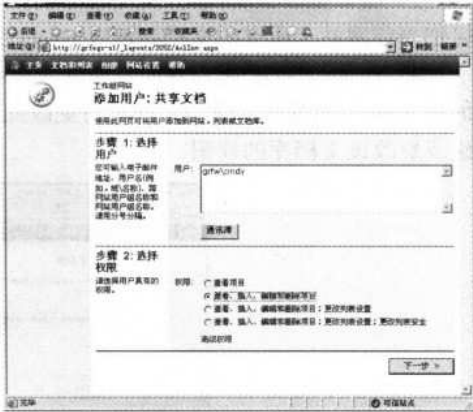


图 9-63 “添加用户—1”界面

单击【下一步】按钮，打开如图 9-64 所示界面。在“步骤 3：确认用户”栏的“电子邮件地址”文本框中输入该用户的电子邮件地址；然后在“步骤 4：发送电子邮件”栏中输入要发送通知的电子邮件地址和通知消息。

最后单击【完成】按钮即开始向所指定的用户发送通知邮件，返回到如图 9-62 所示界面中即可见到新添加的用户及所配置的相应权限，如图 9-65 所示。



图 9-64 “添加用户—2”界面



图 9-65 添加新用户后的“更改权限”界面

如果要对现有用户的权限进行编辑、更改，则可直接单击相应用户链接，在打开的界面中进行修改。

3. 新建文档库和表单库

除了可以使用默认的文档库外，还可以自己创建新的文档库。

(1) 在如图 9-51 所示界面中单击【创建文档库】按钮，打开如图 9-66 所示界面。使用此网页可向此网站添加新文档库。

(2) 单击【文档库】按钮，打开如图 9-67 所示界面。使用此网页可定义此文档库的常规设置。可以设置名称、说明或进行其他设置，如是否将指向此文档库的链接显示在主页中的“快速启动”栏上。配置好文档库名称、是否放置在“快速启动”栏，以及设置好文档版本和所选用的文档模板等后，单击【创建】按钮完成新文档库的创建。新创建的文档库会在“文档和列表”界面中显示，如图 9-68 所示。



图 9-66 “创建网页”界面



图 9-67 “新建文档库”界面

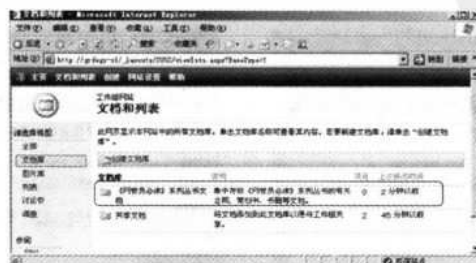


图 9-68 “文档和列表”中显示的新创建文档库

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(3) 如果要创建表单库，则在如图 9-66 所示页中单击【表单库】按钮，打开如图 9-69 所示界面。使用此网页可定义此表单库的常规设置。可以设置名称、说明或其他设置，如是否将指向此表单库的链接显示在主页中的“快速启动”栏上。



图 9-69 “新建表单库”界面

配置好表单库名称、是否放置在“快速启动”栏，以及设置好表单版本和所选用的表单模板等后，单击【创建】按钮完成新表单库的创建。新的表单库的创建同样可以在“文档和列表”界面中显示，如图 9-70 所示。



图 9-70 “文档和列表”中显示的新创建表单库

新建文档和表单库后即可向其中添加文档或表单了。分别在如图 9-68 所示和图 9-70 两界面中单击相应的文档库或表单库，即可打开相应添加文档或表单的界面，分别如图 9-71 所示和图 9-72 所示。图 9-71 所示新文档库的文档新建、添加的方法与前面介绍的文档新建、添加的方法一样，不再赘述。图 9-72 所示的表单库表单新建、添加的方法与文档新建、添加的方法类似，参照即可。

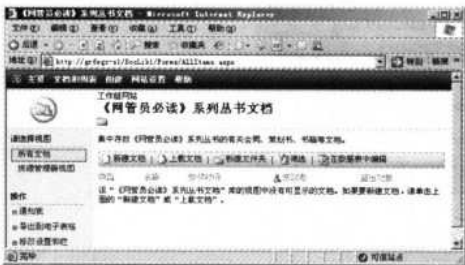


图 9-71 新文档库界面

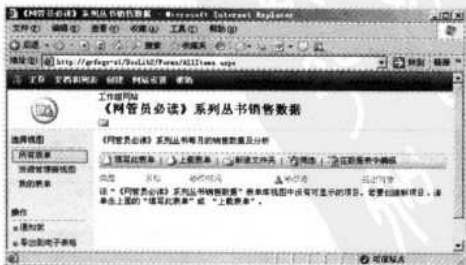


图 9-72 新表单库界面

9.4.3 SharePoint 网站图片库配置与使用

SharePoint 网站的图片与共享文档库一样，都是供网站用户共享的。当然如果不需要图片库，也可以不配置。

(1) 在如图 9-70 所示界面的左边导航栏中单击“图片库”链接，打开如图 9-73 所示界面。此网页显示本网站中的所有图片库。单击图片库名称可查看其内容。



图 9-73 “文档和列表”界面

(2) 单击【创建图片库】按钮，打开如图 9-74 所示界面。使用此网页可向此网站添加新图片库。

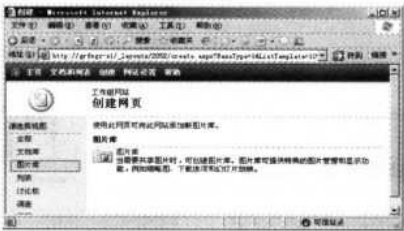


图 9-74 “创建网页”界面

(3) 单击【图片库】按钮，打开如图 9-75 所示界面。使用此网页可定义此图片库的常规设置。可以设置名称、说明和其他设置，如是否将指向此图片库的链接显示在主页中的“快速启动”栏上，以及设置图片版本等后，单击【创建】按钮完成新图片库的创建。新创建的图片库也将显示在“文档和列表”界面中，如图 9-76 所示。



图 9-75 “新建图片库”界面



图 9-76 “文档和列表”中显示的新建图片库

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

588 网管员必读——网络应用（第2版）

新建了图片库后也可以向其中添加图片，方法是在图 9-76 中单击相应的图片库，打开如图 9-77 所示界面。

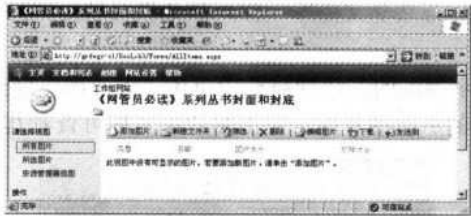


图 9-77 新图片库界面

单击【添加图片】按钮，打开如图 9-78 所示界面。在“名称”文本框中输入，或者直接单击【浏览】按钮查找所需添加的图片路径。然后单击【保存并关闭】按钮返回到如图 9-77 所示界面。

用同样的方法添加其他图片。最终都将在如图 9-77 所示的图片库界面中显示，如图 9-79 所示。



图 9-78 添加新的图片界面



图 9-79 添加图片后的图片库界面

除了可以添加图片外，还可以新建用于存放图片的文件夹，删除已存放的图片，编辑现有图片等，这些功能都在工具栏中有相应的按钮，不再介绍。通过工具栏中的“下载”功能可以把所选图片下载到用户计算机上；通过“发送到”功能，可以把所选图片通过邮件方式发送给其他用户。

9.4.4 SharePoint 网站列表配置与使用

存储和显示用户可用其浏览器添加的信息的网站组件。需要具备运行 Windows SharePoint Services 或 SharePoint Portal Server 的 Web 服务器。

在相应 SharePoint 网站主页导航栏中单击【列表】（如图 9-80 所示）按钮，打开如图 9-81 所示界面。此网页显示本网站中的所有列表，包括联系人、链接、任务、事件和通知。单击列表名称可查看其内容。下面介绍各列表项的创建与配置方法。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-80 SharePoint 网站主页中的“列表”栏



图 9-81 “文档和列表”界面

(1) 在如图 9-81 所示界面中单击【联系人】按钮，打开如图 9-82 所示界面。使用“联系人”列表可获取工作组成员的有关信息。

(2) 要新建联系人，则在如图 9-82 所示界面中单击【新建联系人】按钮，打开如图 9-83 所示界面。在其中配置相应联系人信息，然后单击【保存并关闭】按钮返回到如图 9-82 所示界面。此时会显示新建的联系人信息，如图 9-84 所示。用同样的方法添加其他联系人。



图 9-82 “联系人”界面



图 9-83 “新建联系人”界面



图 9-84 在“联系人”列表中显示的新建联系人

(3) 在如图 9-81 所示界面中单击【链接】按钮，打开如图 9-85 所示界面。使用“链接”列表可管理指向你的工作组成员感兴趣或觉得有用的网页的链接。

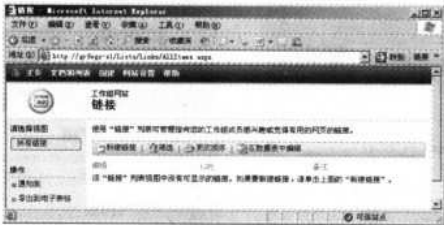


图 9-85 “链接”界面

(4) 单击【新建链接】按钮，打开如图 9-86 所示界面。在“请键入网站地址”文本框中直接输入网站链接地址。然后单击“保存并关闭”按钮完成一个新链接的创建，返回到如图 9-85 所示界面。在其中会显示新创建的链接，如图 9-87 所示。用同样的方法创建其他网站链接。



图 9-86 “新建链接”界面

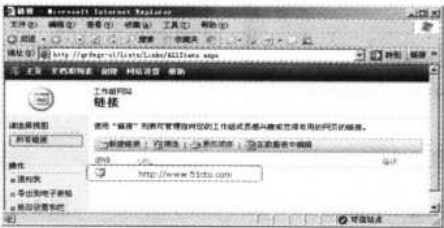


图 9-87 在“链接”列表中显示的新建链接项

(5) 在如图 9-81 所示界面中单击【任务】按钮，打开如图 9-88 所示界面。使用“任务”列表可跟踪用户或工作组需要完成的工作。

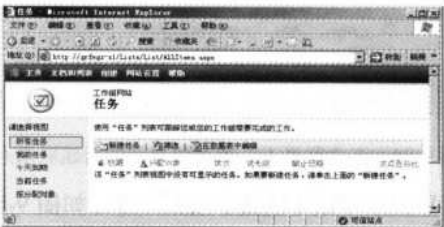


图 9-88 “任务”界面

(6) 单击【新建任务】按钮，打开如图 9-89 所示界面。在“标题”文本框中直接输入任务标题；在“优先级”下拉列表中选择要优先执行的等级；在“状态”下拉列表中选择该任务是否已进行；在“完成百分比”文本框中输入任务的完成百分比；在“分配对象”下拉列表中选择要把该任务分配给哪个用户；在“开始日期”和“截止日期”栏中分别填上任务开始和截止的日期。

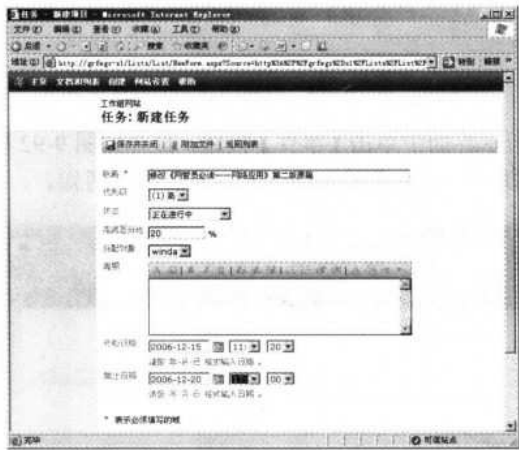


图 9-89 “新建任务”界面

如果要附上要进行的任务的有关文件，则单击工具栏中的【附加文件】按钮，打开如图 9-90 所示界面。在“名称”文本框中输入或者单击【浏览】按钮在打开的窗口中查找要附加的文件路径，然后单击【确定】按钮返回到如图 9-89 所示界面。



图 9-90 附加文件界面

最后在如图 9-89 所示界面中单击【保存并关闭】按钮完成一个新任务的创建，返回到如图 9-88 所示界面。在其中会显示新创建的链接，如图 9-91 所示。用同样的方法添加其他任务。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

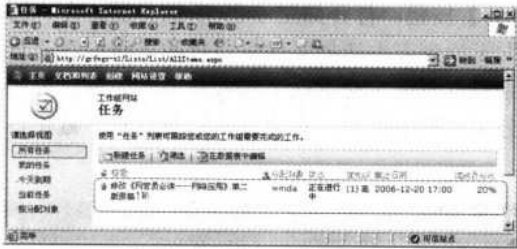


图 9-91 在“任务”列表中显示的新建任务项

(7) 在如图 9-81 所示界面中单击【事件】按钮，打开如图 9-92 所示界面。使用“事件”列表可使自己在会议、期限和其他重要事件即将到来时得到通知。

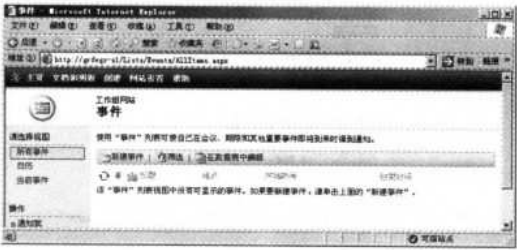


图 9-92 “事件”界面

(8) 单击【新建事件】按钮，打开如图 9-93 所示界面。在“标题”文本框中直接输入事件标题；在“开始时间”和“结束时间”栏中分别填上事件开始和结束的时间；在“重复周期”项下选择事件重复的频率。设置好后单击【保存并关闭】按钮返回到如图 9-92 所示界面，此时会显示新创建的事件，如图 9-94 所示。



图 9-93 “新建事件”界面



图 9-94 在“事件”列表中显示的新建事件项

同样也可以在如图 9-93 中附加与事件有关的文件，附加方法与前面介绍的“任务”列表中附加文件的方法一样，不再赘述。

(9) 在如图 9-81 所示界面中单击【通知】按钮，打开如图 9-95 所示界面。使用该通知列表可在你的网站主页上张贴消息。

(10) 单击【新建通知】按钮，打开如图 9-96 所示界面。在“标题”文本框中直接输入通知标题；在“正文”文本框中输入通知的具体内容；在“截止日期”栏中填上通知截止日期。设置好后单击【保存并关闭】按钮返回到如图 9-95 所示界面，此时会显示新创建的事件，如图 9-97 所示。

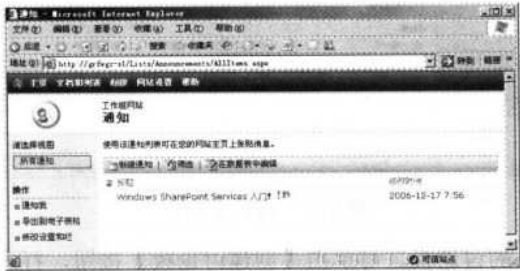


图 9-95 “通知”界面



图 9-96 “新建通知”界面



图 9-97 在“通知”列表中显示的新建通知项

9.4.5 讨论板的配置与使用

讨论板提供了一个论坛，用于工作组交流感兴趣的课题。例如，可以创建一个讨论板供工作组成员提出活动建议，如公司的改革方案、工资、福利待遇政策等。

每个讨论板都显示在一个网页上，该网页包括的按钮可以用来执行以下任务：开始新讨论、排序和筛选讨论、切换到各个讨论板视图和更改讨论板设计。还可以创建通知，以便能在讨论板发生更改时收到通知。可以在顺序化视图或按话题视图中查看讨论、评论。顺序化视图按照创建顺序显示所有评论。按话题视图则按话题显示评论，所有对话话题相同的消息均显示在一起，并按创建顺序排列。

默认情况下，网站自带名为“一般讨论”的内置讨论板，该讨论板位于“快速启动栏”和“文档和列表”网页上。

(1) 在如图 9-81 所示界面中单击【讨论板】按钮，打开如图 9-98 所示界面。此网页显示本网站中的所有讨论板（已内置了一个名为“一般讨论”的讨论板）。单击讨论板名称可查看其内容。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-98 讨论板界面

(2) 如果要创建新的讨论板，可单击【创建讨论板】按钮，打开如图 9-99 所示界面。



图 9-99 “创建网页”界面

(3) 单击【讨论板】按钮，打开如图 9-100 所示界面。使用此网页可定义此讨论板的常规设置。你可以设置名称、说明和其他设置，如是否将指向此讨论板的链接显示在主页中的“快速启动”栏上。



图 9-100 “新建讨论板”界面

在“名称”文本框中输入讨论板的标题名称；在“说明”文本框中输入新建讨论板的简要文字说明；在“导航”栏中选择是否把该讨论板放置在“快速启动”栏上。

设置好后单击【创建】按钮，完成新的讨论板创建，然后显示相应讨论板界面，如图 9-101 所示。

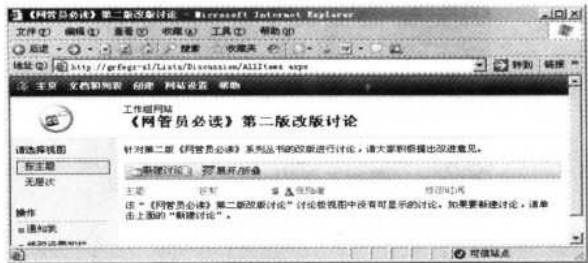


图 9-101 新建的讨论板

用户如果想发帖子，直接单击其中的【新建讨论】按钮，打开如图 9-102 所示界面。在其中输入帖子标题和内容，并可通过单击【附加文件】按钮在打开的对话框中为自己发表的帖子附加文件，完成后单击【保存并关闭】按钮返回到如图 9-101 所示界面。不过此时已新添加了讨论帖子，如图 9-103 所示。



图 9-102 发表讨论板帖子界面

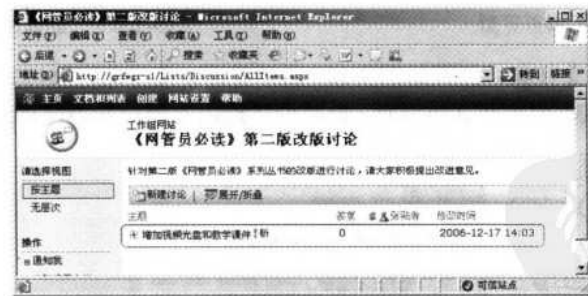


图 9-103 在新建讨论板中的帖子

如果要回复讨论板中的帖子，只需要在如图 9-103 所示界面中单击相应的帖子，在打开的如图 9-104 所示界面中单击【提交答复】按钮，即可在打开的类似如图 9-102 所示的界面中输入回复内容，然后单击【保存并关闭】按钮即可。同样可以通过单击【附加文件】按钮为自己所回复的帖子附加文件。



图 9-104 打开的讨论板帖子

9.4.6 调查项目的配置与使用

调查提供了一种征求工作组成员意见的方式。如果网站包括调查，可以通过单击首页链接栏中的【文档和列表】，再单击【调查】一节中的调查来访问它们。

如果将调查设置为让响应者的姓名可见，则“所有响应”视图可用于查看每个工作组成员响应的方式。“图形摘要”视图则显示响应的汇总。

(1) 在如图 9-81 所示界面中单击【调查】按钮，打开如图 9-105 所示界面。此界面显示本网站中的所有调查，单击调查名称可显示其内容。

(2) 要创建新的调查项目，则可直接单击【创建调查】按钮，打开如图 9-106 所示界面。使用此界面可在此网站添加新调查。



图 9-105 调查界面

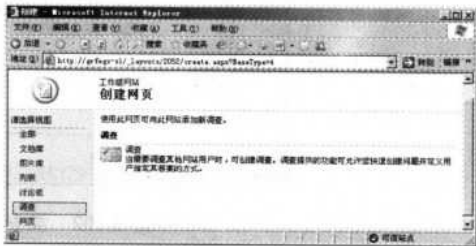


图 9-106 “创建网页”界面

(3) 单击【调查】按钮，打开如图 9-107 所示界面。使用此网页可定义此调查的常规设置。用户可以设置名称、说明和其他设置，如是否将指向此调查库的链接显示在主页中的“快速启动”栏上。



图 9-107 “新建调查—1”界面

在“名称和说明”栏中输入调查的项目名称和简要说明；在“导航”栏中选择是否需要把此调查项目放在导航栏中；在“调查选项”栏中选择是否在调查结果中显示调查的用户名和是否允许多次提交调查结果。

完成后单击【下一步】按钮，进入后面的调查项目设置，如图 9-108 所示（注意，所选择的答案类型的不同，相应界面选项也将不一样）。在这里要选择调查的问题和答案类型，根据实际调查项目输入和选择即可。如果还有其他要调查的问题，则可再次单击【下一步】按钮，再次打开如图 9-108 所示界面，继续输入新的调查问题和答案类型。如果没有其他要调查的问题了，则直接单击【完成】按钮完成调查项目的创建。返回到如图 9-105 所示界面，不过此时已新建了调查项目，如图 9-109 所示。在其中可以继续设置和添加新的调查问题。

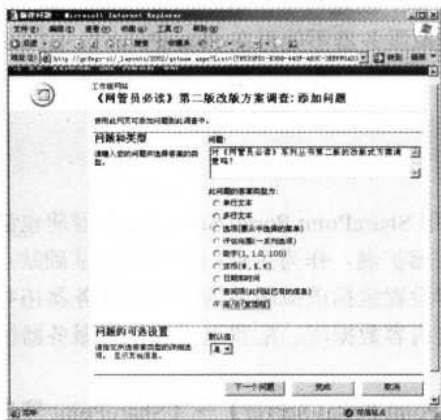


图 9-108 “新建调查—2”界面



图 9-109 新建的调查项目

通过以上各节的介绍，SharePoint 网站的配置就基本上介绍完了，因为篇幅的原因，不可能对网站的各方面设置进行一一介绍。最终的网站主页将显示以上所进行的各项配置，如图 9-110 所示。从中可以快速查看和使用各项应用项目。下面继续介绍 SharePoint Portal Server 2003 服务器的配置方法。



图 9-110 最终设置的 SharePoint 网站主页

9.5 SharePoint Portal Server 2003 服务器的配置

Microsoft Office SharePoint Portal Server 2003 将业务流程中的人员、工作组和知识连接在一起。它将分散的信息统一起来，便于就文档、项目和其他工作进行协作，并根据用户的功能组和组织角色呈现特定应用程序和自定义内容。SharePoint Portal Server 可与 Windows 资源管理器、Office 应用程序和 Web 浏览器协同工作，帮助大家在整个组织范围内创建、管理和共享内容。本节所介绍的操作也必须是网站管理员才具有权限。

借助于 Windows Server 2003、SharePoint Portal Server 与 Office 2003、Windows SharePoint Services 和 Microsoft SQL Server 2000 SP3 集成在一起，创建将整个组织连接起来的统一门户网站。但要注意，在 SharePoint 网站上扩展过的虚拟服务器不能再在 SharePoint Portal Server 门户网站中使用。

9.5.1 SharePoint Portal Server 服务器配置

与 SharePoint Services 服务器一样，在正式使用 SharePoint Portal Server 服务器前也必须进行基本的初始设置。首先要进行的仍是虚拟服务器扩展，作为企业门户网站的基础站点。

本节要介绍的 SharePoint Portal Server 服务器设置包括虚拟服务器扩展、服务器拓扑结构、指定配置数据库、指定组件设置数据库、指定内容数据库、配置电子邮件和服务器场账户（可选）。下面分别予以简单介绍。

（1）执行【开始】→【所有程序】→【SharePoint Portal Server】→【SharePoint 管理中心】菜单操作，首先打开的是如图 9-22 所示界面。在其中配置好电子邮件和虚拟服务器（一定要是没有经过扩展的虚拟服务器）后进入如图 9-111 所示主页。

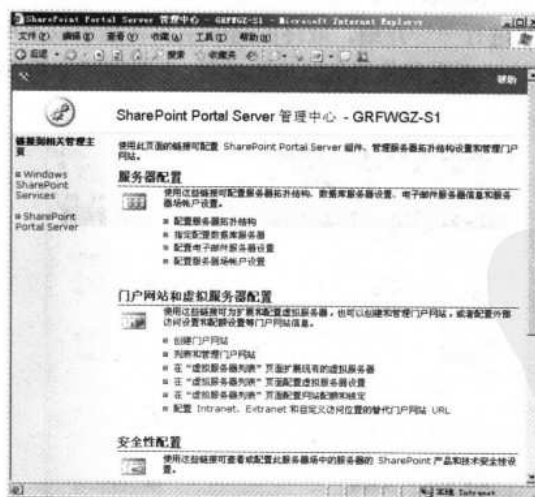


图 9-111 “SharePoint Portal 管理中心”界面

（2）在“服务器配置”栏下单击【配置服务器拓扑结构】链接项，打开如图 9-112 所示界面。使用此界面可查看服务器场中各个服务器上活动的 SharePoint Portal Server 组件、在服

务器场中删除服务器，以及更改各个服务器上的组件。带有*标记的数据库服务器是默认数据库服务器。若要指定各个数据库服务器的设置，请单击服务器名称，在打开的界面中重新配置。“Single Sign-on”服务是针对服务器场环境下启用一项服务，在单 Web 服务器环境中无须配置。

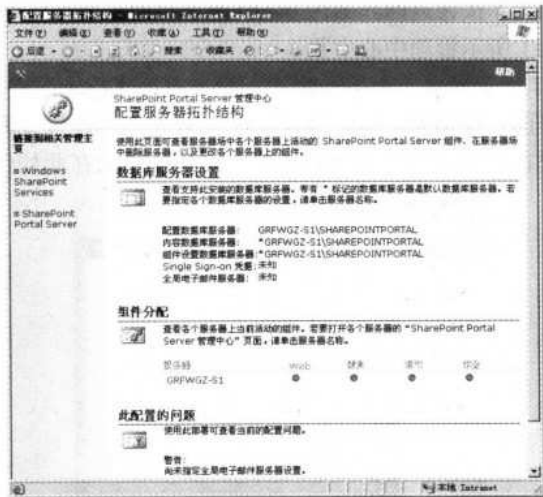


图 9-112 “配置服务器拓扑结构”界面

(3) 单击如图 9-112 所示界面下部的【更改组件】按钮，打开如图 9-113 所示界面。使用此界面可更改各个服务器上的活动组件。



图 9-113 “更改组件分配”界面

在“组件分配”栏中通过选择复选框可为指定的服务器分配组件。可以为每台服务器分配一个或多个组件。在“作业服务器组件”栏中选择一个服务器以运行后台任务。如果更改作业服务器，就必须重新配置 Single Sign-On 服务（在“服务”窗口中启动即可）。但是更改作业服务器将导致从当前作业服务器删除所有内容源和索引。

文档库服务器组件的配置是可选的。不过在键入服务器名称之前，必须先安装向下兼容

600 网管员必读——网络应用（第2版）

的文档库的服务器组件（参见图 9-13 所示）。如果要配置文档服务器，则在“文档服务器”文本框中输入文档管理服务器 URL。如果文档管理服务器上启用了安全套接字层（SSL），URL 必须是 https 地址，例如 https://server_name。如果你不使用 SSL，URL 必须是 http://server_name 或者 server_name。

配置好后单击【确定】按钮返回到如图 9-110 所示界面。最后再单击界面下面的【关闭】按钮可返回到如图 9-111 所示管理中心主页。

（4）在如图 9-111 所示界面“服务器配置”栏下单击【指定配置数据库服务器】链接，打开如图 9-114 所示界面。使用此界面可创建与配置数据库的连接或取消连接。因为相应虚拟服务器的相关设置已在扩展虚拟服务器时设置，所以实际上在此处仅可查看。



图 9-114 “指定配置服务器数据库的设置”界面

单击【确定】按钮可返回到如图 9-111 所示管理中心主页。

（5）在如图 9-111 所示界面“服务器配置”栏下单击【配置电子邮件服务器设置】链接项，打开如图 9-115 所示界面。使用此网页上的设置可配置所有虚拟服务器的默认电子邮件设置。设置好后单击【确定】按钮返回到如图 9-111 所示管理中心界面。

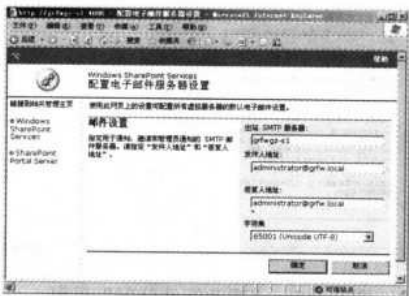


图 9-115 “配置电子邮件服务器设置”界面



因为本章仅以单 Web 服务器为例进行介绍，不介绍服务器场情形，所以在此对于如图 9-111 所示管理中心界面“服务器设置”栏下的“配置服务器场账户设置”选项不作介绍。

9.5.2 创建门户网站

在安装并初始配置服务器之后，即可以创建其他门户网站。具体步骤如下。

(1) 在如图 9-111 所示管理中心界面“门户网站和虚拟服务器配置”栏下单击【创建门户网站】链接，打开如图 9-116 所示界面。



图 9-116 “创建门户网站”界面

(2) 在“网站名称”栏的“名称”文本框中键入门户网站的名称。此名称出现在大多数门户网站界面的顶端。在“网站 URL”栏的“虚拟服务器”列表中选择此服务器上将作为门户网站宿主的现有虚拟服务器，实际上已默认选择了，因为进入 SharePoint Portal Server 配置的开始就需要选择虚拟服务器；在 URL 文本框中键入用户用于连接门户网站的 URL。默认情况下，此 URL 为 http://server_name/。如果选择端口号不等于 80 的虚拟服务器，端口号将显示为 URL 的一部分，例如此处笔者的 http://grfwfwgz-s1:8088/。

注意 此处所选择的虚拟服务器一定要是未被除数扩展过（包括在 SharePoint Services 服务器上的扩展）的虚拟服务器，否则会显示“没有可用的虚拟服务器，或者选中的虚拟服务器已被扩展。”的错误提示。

(3) 在“所有者”栏的“账户名”文本框中以“域\用户名”格式键入门户网站所有者的账户名。门户网站所有者负责管理内容和用户访问。在“电子邮件地址”文本框中键入门户网站所有者的电子邮件地址。

(4) 单击【确定】按钮完成新门户网站的创建，打开如图 9-117 所示界面。再次单击【确定】按钮开始创建门户网站，将出现“操作状态”页，如图 9-118 所示。

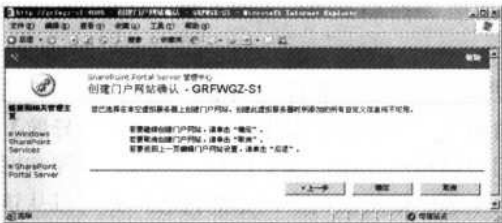


图 9-117 “创建门户网站确认”界面

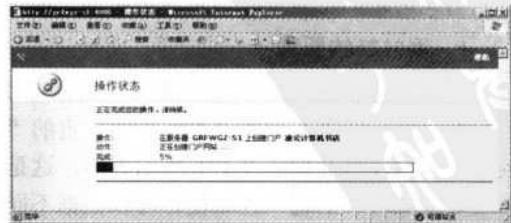


图 9-118 “操作状态”界面

602 网管员必读——网络应用（第2版）

成功创建门户网站之后，将出现“操作成功”界面，如图 9-119 所示。在其中显示了该门户网站的地址和管理界面地址。现在就可以正式利用所给出的网站地址访问门户网站了，如图 9-120 所示。当然，最好还是先按如图 9-118 所示的提示进行进一步的配置。

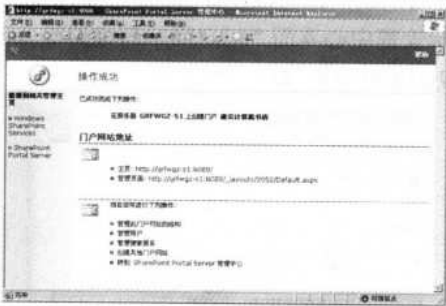


图 9-119 门户网站创建成功的提示界面



图 9-120 SharePoint Portal Server 配置的门户网站示例



注意

一旦开始创建门户网站，任何添加到虚拟服务器的自定义内容都将不可用。若所选择虚拟服务器与其他虚拟服务器是同一个目录，则也不能创建成功，会显示诸如“无法创建门户，因为该虚拟服务器选定的目录已被其他虚拟服务器（XXX）使用。”的错误提示。

9.5.3 门户网站的配置

门户网站的配置主要包括网站结构、网站的用户管理两方面。下面分别予以介绍。

1. 网站结构配置

(1) 在如图 9-119 所示界面“现在你可以进行下列操作”栏中单击【管理此门户网站的 结构】链接，或者在如图 9-120 所示主页的“自定义门户”栏下单击【更改门户网站导航】链接，都可以打开如图 9-121 所示界面。这是门户结构的视图，其中包括：主题、新闻和网站三大区域。“主题”区域使你可以根据不同的主题区域组织门户网站的内容，并可以从该页开始浏览并查找感兴趣的主题。“新闻”区域包含有关的组织的新闻，列表中显示的是按

日期组织的新闻项目列表。“网站”区域列出了与该门户网站相关的网站。你可根据其属性浏览网站、搜索网站，以及在“聚焦网站”中搜索感兴趣的网站。

在这个结构视图中，可以从此视图将区域和列表拖动到新的位置。还可以通过单击区域菜单上的【筛选器】按钮将视图仅限制为当前区域。若要返回整个列表，请单击【重置】按钮。为了使大家对“区域”这个概念有一个更清楚的认识，下面比较详细地介绍一下 SharePoint Portal Server 2003 系统中的这个术语。

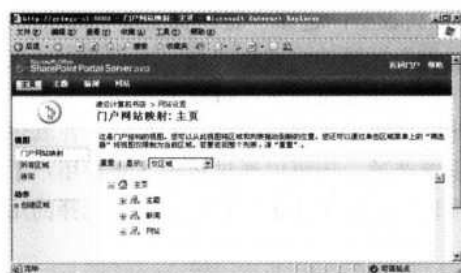


图 9-121 “网站门户映射: 主页”界面

Microsoft Office SharePoint Portal Server 2003 中的门户网站区域提供了直观的导航工具，以查找和浏览所有类型的内容（从文档到人员，再到基于 Windows SharePoint Services 的网站）。通过使用区域将内容分组，可以对门户网站中的信息进行组织。这就使用户可以浏览信息。“主题”下面的区域能够帮助不熟悉门户网站其他区域的用户找到所需信息。一个文档可以出现在多个不同区域中。区域可以包括存储在 SharePoint Portal Server 中的文档和指向其他内容源（例如网站或文件共享）信息的链接。创建有效的门户网站结构需要进行规划，并对其他人组织内容的方式有一定的了解。

在 SharePoint Portal Server 中，区域具有两个作用。第一，它们提供门户网站和相关内容的导航结构或映射。通过添加、移动或删除区域，可以更改用户门户网站的视图。第二，它们提供信息浏览的集中结构。在有组织的主题层次结构中，区域可将读者指引到他们要寻找的信息中去。区域提供了一种描述和寻找文档的灵活方式。

作为网站管理员，你可以向内容管理者网站用户组中添加用户。默认情况下，内容管理者可以批准或拒绝内容请求、管理区域设置，以及向此区域的网站用户组中添加用户。此外，网站管理员或内容管理者还可以指定由一个或多个访问群体查看的目标区域。

区域提供门户网站和相关内容导航结构或映射。通过添加、移动或删除区域，可以为用户更改门户网站的视图。“主页”区域下的顶层区域构成门户网站的主导航。如果将区域移至该层，它就会显示在导航栏上。门户网站映射使你可以拖动区域和列表以更改门户网站的导航结构或内容组织。

区域还提供信息浏览的集中结构。它们指导读者通过内容层次结构查看他们所查找的信息。主题专家可以使用区域组织和发布有关特定主题的信息。要创建协作环境，可以添加列表、讨论板、文档库，以及使用户能够协同工作的其他功能。为便于查找，你可以向多个区域中添加项目或列表。

如果具有大量内容，按主题对它们进行划分可能是一项极为耗时的工作。为了简化该过程，Microsoft Office SharePoint Portal Server 2003 提供了一种称为“主题助手”的自动工具。

向每个主题分配几个具有代表性的项目后，“主题助手”会将这些示例项目与未被分配的项目进行比较，然后自动选择最佳匹配的主题。

门户网站的“管理员”网站用户组的成员可以向“内容管理者”网站用户组中分配用户。默认情况下，“内容管理者”网站用户组的成员可以批准或拒绝内容请求，以及管理区域设置。另外，作为网站管理员或内容管理者，你可以指定由一个或多个访问群体进行查看的目标区域。可以对图 9-118 所示界面中的区域进行一一配置，还可创建新的区域和各区域列表。

(2) 单击“主题”下拉列表框，选择“管理安全性”选项，打开如图 9-122 所示界面。

使用该界面可管理“主题”区域的网站用户组、用户或组的安全设置。所有用户都可以在导航结构上看到此区域，但仅向具有查看区域权限的用户显示。这些是从父区域继承的权限。如果更改这些权限，此区域将不再继承父区域的权限。在其中选择各种用户可以查看和其他权限访问“主题”的设置选项，还可以通过单击【新建用户】按钮来创建新的允许访问“主题”的用户账户。当然也可以通过【编辑】按钮对所选择的用户对象权限进行编辑，而不是按系统默认的设置。

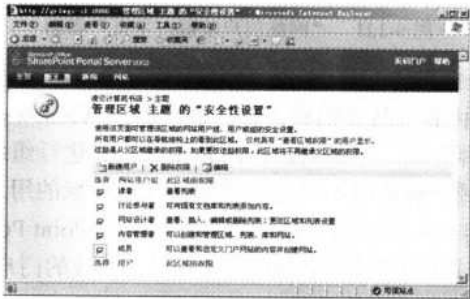


图 9-122 管理区域“主题”的安全性设置界面

(3) 在如图 9-121 所示界面的“主题”区域下拉列表框中选择“创建子区域”选项，打开如图 9-123 所示界面。在其中配置相关子区域子设置，然后单击【确定】按钮即可返回到如图 9-121 所示界面，不过此时新添加了子主题区域。



图 9-123 “创建区域”界面

也可以通过单击如图 9-123 所示界面底部的【更改位置】链接，打开如图 9-124 所示界面，在其中重新选择该新建的子区域所在的位置。然后单击【确定】按钮即可完成新区域的创建。



其实在“主题”区域中系统已内置了许多子区域，其中包括：部门、资源、战略、项目等，如图 9-125 所示。在这些子区域下也可以继续创建自己的子区域和列表。创建的方法是一样的，不再赘述。



图 9-124 “更改位置”界面



图 9-125 系统内置的“主题”区域下的子区域

(3) 在如图 9-121 所示界面的“主题”区域下拉列表框中选择“创建列表”选项，打开如图 9-126 所示界面。使用本界面可将列表添加到区域中。在显示此区域中的列表之前，可能需要批准列表。

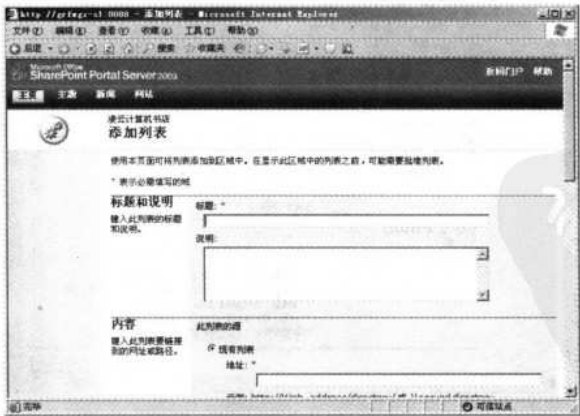


图 9-126 “添加列表”界面

在其中要设置列表名称、列表文件所在路径、列表所分配的组、访问群体等选项。因为其他区域的配置方法与“主题”区域的各项配置方法一样，在此不再赘述。下面介

绍门户网站的管理用户。

2. 管理用户配置

在如图 9-119 所示界面中单击【管理用户】链接，打开如图 9-127 所示界面。使用此界面可添加新用户、从所有网站用户组中删除用户或将用户分配到网站用户组。若要编辑用户属于哪些网站用户组，请在列表中单击用户名。

要为门户网站添加新的用户，则单击【添加用户】按钮，打开如图 9-128 所示界面。在“步骤 1：选择用户”文本框中按提示的格式输入用户账户；在“步骤 2：选择网站用户组”栏中选择该用户所属的网站用户组，其实也就是该用户对网站的访问权限设置。

单击【下一步】按钮，打开如图 9-129 所示界面。如果所添加的用户不是此网站的成员，在“步骤 3：确认用户”栏中输入用户的电子邮件地址，系统将按照在此处提供的信息将他们自动添加到网站。在“步骤 4：发送电子邮件”栏中可发送显示在此网页上的电子邮件。

最后单击【完成】按钮完成新用户的创建。

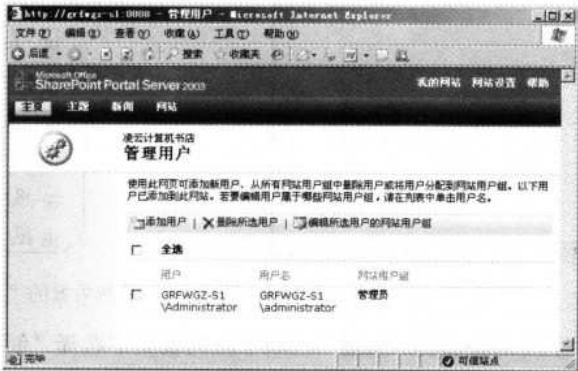


图 9-127 “管理用户”界面

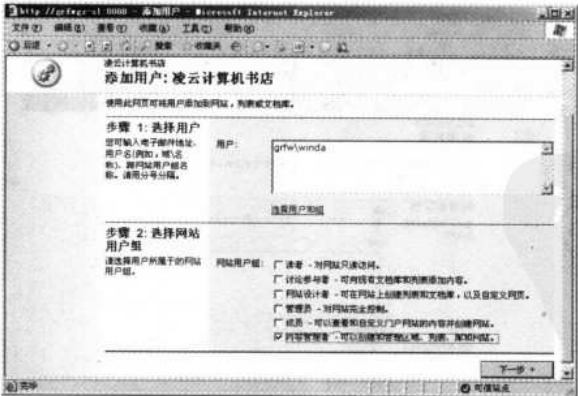


图 9-128 “添加用户—1”界面



图 9-129 “添加用户—2”界面

9.5.4 配置门户网站安全性

门户网站包括潜在的敏感信息，如账户名或组织信息。为防止数据遭到网络入侵及检测，需要部署一定的安全设置。在 Microsoft Office SharePoint Portal Server 2003 中，网站用户组可以提供灵活的方法来帮助控制对内容的访问。网站用户组是基于用户执行任务的种类来为其配置权限的方法。SharePoint Portal Server 在搜索期间可以识别组织机构服务器、文件共享和数据库上使用的安全策略。安全性是非常重要的，它有助于防止用户在门户网站执行搜索时查找他们无权访问的文档。

在门户网站中，SharePoint Portal Server 使用默认网站用户组将具有一组特定的可自定义权限的用户进行分组。也可以为特定区域或列表创建自定义网站用户组，并且为其分配一组特定的权限。此外，默认情况下，SharePoint Portal Server 使用 Windows SharePoint Services 提供的默认网站用户组。

下面简单介绍一下门户网站安全性的配置。

1) 创建 Windows 组

为将拥有相同一组权限的用户创建 Windows 组。例如，可以为拥有一组权限的全部作者创建一个组，而为拥有另一组权限的市场部门创建另一个组。

2) 将组分配到网站用户组

将以上各个组分别分配给六个默认的 Microsoft SharePoint Portal Server 网站用户组。

- 读者：拥有在门户网站上查看项目和使用搜索的权限。
- 成员：拥有读者权限，外加添加项目、个性化 Web 部件、使用通知及创建个人网站的权限。
- 讨论参与者：拥有成员权限，外加添加及编辑项目、管理列表权限、管理个人组和视图，以及个性化 Web 部件页的权限。讨论参与者不能新建列表或文档库，但可以将内容添加到现有列表和文档库中。
- 网站设计者：拥有讨论参与者权限，外加取消签出、删除项目、管理列表、添加及自定义网页、定义及应用主题和边框，以及链接样式表的权限。网站设计者可以修

608 网管员必读——网络应用（第2版）

改网站结构，并新建列表或文档库。

- 管理员：具有其他所有网站用户组的权限，外加管理网站用户组及查看使用情况分析数据的权限。“管理员”网站用户组无法自定义或删除，而且必须始终至少拥有一个成员。该组成员始终都具有访问网站中任何项目的权限，也可以为自己授予这种权限。
- 内容管理者：具有管理某个区域中全部设置或内容的权限。内容管理者可以批准或拒绝提交请求，以及将内容移动到存档及更改安全性。

为网站用户组添加组而不是添加单独用户是一种更为灵活的配置安全性的方式，当组成员身份更改时，会自动在网站用户组成员身份中反映出来。

3) 编辑网站用户组权限

转到网站用户组管理页以确保分配给默认网站用户组的权限就是希望分别分配给这些组的权限。若要转到这些网页，请执行下列操作。

- (1) 在门户网站主页顶端单击【网站设置】按钮，打开如图 9-130 所示界面。在“常规设置”栏中单击【管理安全性和附加设置】链接，打开如图 9-131 所示界面。
- (2) 在“管理安全性和附加设置”页上的“用户和权限”栏中单击【管理网站用户组】链接，打开如图 9-132 所示界面。



图 9-130 “网站设置”界面



图 9-131 “管理安全性和附加设置”界面

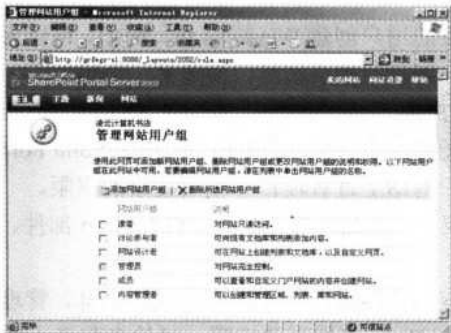


图 9-132 “管理网站用户组”界面

- (3) 在“‘网站用户组’成员”页上，单击要编辑权限的用户组，打开如图 9-133 所示界面。



图 9-133 “成员所属跨网站用户组: ‘读者’”界面

(4) 单击【编辑网站用户组权限】按钮，打开如图 9-134 所示界面。在这时重新配置相应用户组所拥有的权限。完成后再单击界面底部的【确定】按钮（图中未显示）完成权限配置。用同样的方法可以编辑其他用户组的权限。



图 9-134 “更改网站用户组权限”界面

4) 自定义区域的安全性

可以为每个区域自定义安全性。建议管理员在自定义区域安全性之前为网站用户组添加组，从而避免出现安全策略不一致的现象。在父区域设置安全性，这些设置也会应用于其全部子区域。如果在子区域上自定义安全性，就会破坏继承。子区域将不再继承对父区域进行的更改。

要授予用户对某一区域的完全控制权限，包括自定义 Web 部件和 Web 部件页的权限，请确保该用户还是整个网站范围的“讨论参与者”网站用户组的成员。要转到某一区域的“管理安全性设置”页，请单击导航栏中的“管理安全性”按钮，如图 9-135 所示界面是“主题”区域中的“管理安全性”选项。打开后的界面如图 9-136 所示。



图 9-135 “主题”区域中的“管理安全性”选项



图 9-136 “管理区域主题的安全性设置”界面

5) 防止成员创建个人网站

默认情况下，“成员”网站用户组的成员授予了创建个人网站（我的网站）的权限。除“读者”用户组之外的全部网站用户组都可以创建个人网站。如果希望取消此权限，请从“读者”网站用户组复制权限，并使用这些权限（查看区域、查看界面及搜索）创建新的网站用户组。然后将用户组或单个用户分配至此新建网站用户组，取消其中的“创建个人网站”权限（参见图 9-134 所示界面），即可避免他们创建个人网站。

9.5.5 为门户网站添加 SharePoint 站点

可使用顶级网站和子网站将网站内容划分为明确的、单独的可管理网站。顶级网站可以拥有多个子网站，而这些子网站也可以拥有多个子网站，可根据用户需要向下建设无限层次的子网站。顶级网站和其所有子网站所组成的整个结构称为 Web 网站集。如图 9-137 所示显示了网站和子网站的这种层次结构。

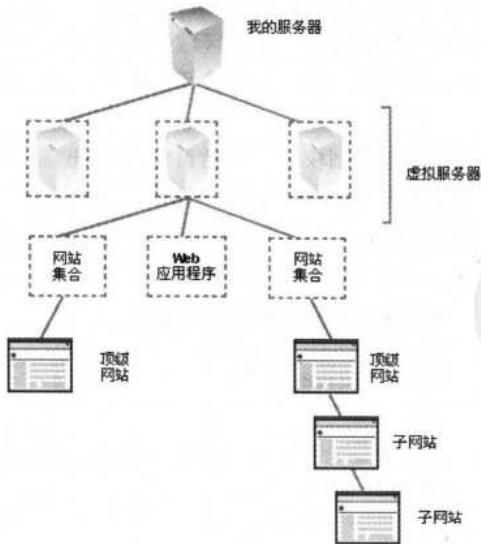


图 9-137 SharePoint 网站和子网站的关系

通过这种层次结构，用户可以有一个用于整个工作组的主工作网站，外加各个工作网站或

用于从属项目的共享网站。顶级网站和子网站允许对网站功能和设置进行不同级别的控制。

网站集的管理员可以控制顶级网站及其下所有子网站的设置和功能。

- 添加、删除或更改用户权限。
- 使用情况统计信息。
- 更改区域设置。
- 管理 Web 部件和模板库。
- 管理 Web 讨论和通知。
- 更改网站的名称及说明、主题和主页组织形式。
- 配置顶级网站和所有子网站的相关设置，如区域设置。

子网站的管理员只能控制该子网站的设置和功能，而下一级子网站的管理员只能控制该子网站的设置和功能。

- 添加、删除或更改用户权限（如果已设置唯一权限）。
- 查看使用情况分析数据。
- 更改区域设置。
- 管理 Web 讨论和通知。
- 更改网站的名称及说明、主题和主页组织形式。

在本章的前面就说到，SharePoint Portal Server 企业门户网站可以集成 SharePoint Services 站点（当然也可以不是 SharePoint Services 站点，只是普通网站），为企业提供一个统一的信息化入口。添加网站有两种途径：一是直接添加网站链接；另一种是直接创建新的 SharePoint 站点。下面分别介绍具体的添加方法。

1. 向网站中添加站点链接

(1) 在门户网站的主页顶部单击【网站】按钮，打开如图 9-138 所示界面。



图 9-138 “网站”界面

(2) 在左边导航栏中单击【向网站添加链接】按钮，打开如图 9-139 所示界面。使用本界面可向“网站目录”添加网站链接。这使用户可以利用该网站搜索或浏览网站。

612 网管员必读——网络应用（第2版）



图 9-139 “向网站添加链接”界面

在“网络链接”栏的“标题”文本框中输入要链接网站的地址；在“URL”文本框中输入该链接网站的地址；在“说明”文本框中输入该链接网站的简要说明；在“所有者”文本框中输入该链接网站的所有者，同样要以“域\用户账户”的格式输入；在“部门”下拉列表框中选择该链接网站所属部门（也可不选）；在“地区”下拉列表框中选择该链接网站的类型（也可不选）；如果把该链接网站作为门户网站的主要站点，则选择“聚集网站”复选项。

在“搜索结果”栏中根据需要选择“在搜索结果中包含”复选项。如果要更改链接网站所在的区域位置，可单击“区域”栏中的【更改位置】链接重新选择所属的位置，可以在“主题”、“新闻”和“网站”三大区域中选择。

设置完成后单击界面底部的【确定】按钮（图中未显示）完成一个网站的链接。新链接网站将在界面显示，如图 9-140 所示。



图 9-140 在“网站”界面中显示的新网站链接

2. 创建新的顶级 SharePoint 网站

除了可以向门户网站中添加已有网站的链接，还可以自己创建顶级 SharePoint 网站。默认情况下，Microsoft Office SharePoint Portal Server 2003 支持直接从门户网站创建基于 Windows SharePoint Services 的网站。这些网站为人们的工作组交流、共享文档，以及共同完成项目提供了场所。默认情况下，每个网站模板都有来自 Windows SharePoint Services 的一组自定义协作功能。

SharePoint Portal Server 含有满足业务需要的各种模板。用户可以从这些模板中选择模板，以便创建最符合项目的网站。例如，可以创建可促进文档协作的文档工作区网站，创建便于计划和跟踪会议的会议工作区网站，创建用来就特定项目进行协作的网站，等等。

创建新的顶级网站方法是在如图 9-138 所示页面左边导航栏中单击【创建网站】按钮，打开如图 9-141 所示界面。使用此界面可新建顶级 SharePoint 网站。用户可指定标题、网站地址、网站所有者的电子邮件地址。



图 9-141 “新建 SharePoint 网站”界面

在“标题”文本框中输入新的顶级网站标题；在“说明”文本框中输入新网站的简要说明（可选）；在“网站地址”栏中的“URL 名称”文本框中输入新的顶级网站的二级 URL 名称；在“电子邮件地址”文本框中输入新网站所有者的电子邮件地址。

设置好后单击【创建】按钮后打开如图 9-142 所示界面，它与向网站中添加网站链接的图 9-131 界面基本一样。也是需要配置网站所属部门、地区和对应的区域位置等选项。设置好后单击【确定】按钮，打开如图 9-143 所示界面，要求为新的顶级网站选择网站模板。然后再单击【确定】按钮进入新的顶级网站主页，如图 9-144 所示。需要重新按本章前面介绍的 SharePoint 站点配置方法对新的网站进行配置。

此时在如图 9-130 所示“网站”界面中可以见到新添加的顶级网站，如图 9-145 所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 9-142 “向网站添加链接”界面



图 9-143 “模板选择”界面



图 9-144 新的顶级网站主页



图 9-145 在“网站”界面中显示的新顶级网站

9.5.6 为门户网站添加个人网站

除了可以创建顶级网站外，用户自己还可以创建名为“我的网站”的个人网站。当用户首次在门户网站的主页上单击【我的网站】按钮（如图 9-146 所示）时，会创建个人网站。



图 9-146 “我的网站”按钮

“我的网站”是通过门户网站查看及参与组织内的 Intranet 的个人起始位置。它为保存和共享工作提供了场所，为找到和联系组织中其他人员及查看他们的工作提供了方法，也为

自定义组织中其他人员查看你的工作的方式提供了方法。若要查看“我的网站”，请单击门户网站顶部的【我的网站】按钮，首先会打开一个如图 9-147 所示的提示框，单击【确定】按钮，随即会生成相应用户的个人网站，如图 9-148 所示。

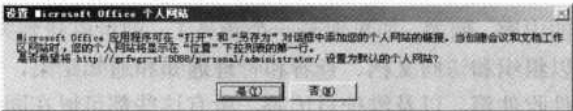


图 9-147 创建个人网站时的提示框



图 9-148 新创建的个人网站

- 同其他大多数 SharePoint 网站一样，你的个人网站含有带下列链接的首页链接栏。
- 首页：此链接将带你返回个人网站的主页。如果是你的个人网站，看到的将是个人视图。如果是其他人的个人网站，看到的将是公共视图。
 - 文档和列表：此链接显示你个人网站的所有列表，及每个列表中的文档数。你还可以从该页创建各种类型的列表。
 - 网站设置：此链接为你的个人网站提供管理、自定义及信息管理页。
 - 帮助：此链接显示当前页的帮助。

原来经常在 SharePoint 网站首页的链接栏中看到的【创建】链接，个人网站的个人视图的动作栏中已经替换为【创建列表】和【创建网页】链接。你可以通过创建各种类型的列表和新的 Web 部件页扩展个人网站，还可以选择是否与组织中其他人员共享列表或网页。

要为个人网站上的任何网页添加、移除或修改 Web 部件，请单击首页右上角的【修改我的网页】下拉菜单，或者单击任一 Web 部件右边向下箭头，在弹出菜单中选择【修改我的 Web 部件】命令，如图 9-149 所示。



图 9-149 Web 部件中的【修改我的 Web 部件】菜单项

616 网管员必读——网络应用（第2版）

1. 个人网站的用途

1) 通过“我的网站”查看信息

个人网站中有一个个人视图，其中包含你所感兴趣的信息。此视图包含基于你的特定访问群体身份为你指定的内容。例如，如果你是一个新员工，则可以找到关键培训资源的链接。通过个人视图，还可以组织和访问文档、查看和管理通知和通知结果，链接到感兴趣的人员和信息、查看电子邮件收件箱，以及维护日历等，所有这些都可以在同一场所完成。

2) 通过“我的网站”共享信息

个人网站中有一个公共视图，其中包含与其他用户共享的信息。用户配置文件的公共属性，连同认为其他用户可能需要查看的链接和网站都显示在此界面上。最近共享的文档也会自动显示在个人网站的公共视图中。

使用个人网站的公共视图，可以方便地管理组织中的其他人查找你及你工作的方式。你可以很容易地更新你的公共配置文件，提供适当的共享链接及共享文档和其他信息，并可以将指向你网站的链接发送给组织中的其他人。

你网站的公共视图并不是你与其他用户共享信息的唯一场所。你的个人网站还包括 Microsoft Windows SharePoint Services 网站的所有功能。可以创建文档和图片库、日历、调查、任务及其他 SharePoint 列表；可以在个人网站上创建其他界面并在你网站的公共视图上提供指向这些界面的链接。将在个人网站中创建的任何文档添加到公共文档库后，便可以与其他用户共享这些文档。

3) 通过“我的网站”查找用户

就像通过个人网站的公共视图与组织中的其他人共享信息一样，你还可以通过其他人的个人网站的公共视图找到他们并与之联系。用户名显示在门户网站中时，单击该名称可以查看该人员个人网站的公共视图。你可以查看人员选择共享的所有内容，可以查看指向网站、人员和文档的人员共享链接，以帮助你完成自己的工作，此外也可以查看彼此共有的信息。

2. 配置个人网站

根据网站管理员授予的权限，可以通过添加和删除 Web 部件、更改 Web 部件在个人网站的个人视图中的布局和外观来自定义个人网站信息，并在操作窗口中添加指向某种信息的链接。

网站管理员可以确定用户在“我的网站”中具有个性化级别。他们可以定义用户向其网页添加的 Web 部件数量和范围，以及用户在何种情况下可以添加或删除这些 Web 部件。他们可以修改“我的网站”的共享视图，从而自定义个人网站的默认外观。如果他们具备“管理访问群体”权限，则还可以根据用户的特定访问群体身份为他们指定内容。

你可以通过更改布局或通过添加、删除或修改任意网页的 Web 部件来自定义个人网站。要在个人网站上修改网页，请单击首页的【修改我的网页】下拉菜单下任意 Web 部件上的【修改我的 Web 部件】命令，菜单项如图 9-150 所示。如图 9-151 所示的是修改“您的新闻”Web 部件窗口。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

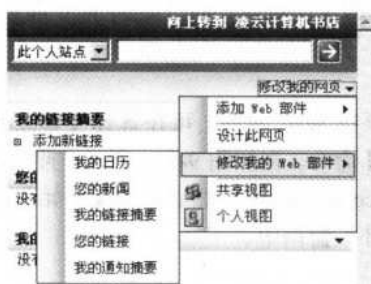


图 9-150 【修改我的网页】下拉菜单



图 9-151 修改“您的新闻”Web 部件窗口

默认情况下，只能对个人视图的 **Web** 部件页进行更改。**Web** 部件页的管理员可以修改该页的共享视图，所有能查看该页的人员都可以看到所作的更改。

要修改 Web 部件页的共享视图，请单击首页的【修改我的网页】下拉菜单中的【共享视图】命令，然后按照说明进行所希望的更改。

要修改 Web 部件页的个人视图，请单击首页的【修改我的网页】下拉菜单中的【个人视图】命令，然后按照说明进行所希望的更改。



如果具有管理员权限,则可以对“我的网站”主页上个人视图的共享视图进行修改。这些修改对所有用户的个人网页的个人视图都有效。如果修改的是主页的个人视图,则修改仅对你的个人网站的个人视图有效。如果不具有管理员权限,则不能对“我的网站”主页的共享视图进行修改。

还可修改网页的布局，方法是在如图 9-150 所示的【修改我的网页】拉菜单中单击【设计此网页】单选项，打开如图 9-152 所示界面。



图 9-152 执行【设计此网页】菜单项打开的界面

现在处于 Web 部件页设计模式，再次单击【设计此网页】可返回此页的普通视图。在此页中拖动 Web 部件，以对它们进行排列。

行远程管理。另外，通过使用命令行界面或者 HTML 管理页还可以设置属性，如指定是否为虚拟服务器启用通知。

1. HTML 管理方式

Windows SharePoint Services 包括的“HTML 管理”页可帮助你管理网站和服务。可以在本地服务器计算机上使用这些表单，也可以从连接 Internet 的远程计算机使用这些表单。必须具有管理员权限才能使用“HTML 管理”页。

对于 Windows SharePoint Services，有“管理中心”页和“网站设置”页两种类型的管理页。“管理中心”页使你能够管理 Web 服务器和虚拟服务器的设置。这些网页是在安装 Windows SharePoint Services 过程中创建的。默认情况下，新创建的虚拟服务器会继承“管理中心”页上的默认设置。可以更改这些默认设置，并指定每一个扩展虚拟服务器使用什么设置。必须是服务器计算机的本地管理员组成员或 SharePoint 管理员组成员，才能查看“管理中心”页。

“管理中心”页存储在 Windows SharePoint Services 在安装过程中所创建的管理端口上。若要查看这些网页。请执行【开始】→【管理工具】→【SharePoint 管理中心】菜单操作，或者从远程计算机的浏览器键入该管理端口上这些网页的 URL。例如：<http://servername:port>（这时原 port 端口号不是固定的），要查看你自己的 SharePoint 管理中心网站所用的端口号，如图 9-155 所示。



图 9-155 “SharePoint 管理中心”属性对话框中的“网站”标签

除了“管理中心”页（该网页控制每个服务器和虚拟服务器的设置）之外，还有几个管理网页可控制每个网站的设置。可以从“网站设置”页执行某些管理性操作，并且可以从此处连接到“顶级网站管理”网页。必须对网站具有管理员权限才能在“网站设置”和“顶级网站管理”页上执行管理性操作。

在“网站设置”和“顶级网站管理”页，可以执行如下任务。

- 管理用户和网站用户组：可以添加或删除用户、编辑网站用户组，以及更改用户的网站用户组成员身份。
- 创建或删除子网站：可以添加子网站或管理网站的现有子网站。
- 更改匿名访问：如果包含网站的虚拟服务器可使用匿名访问，则可以控制是否对网

620 网管员必读——网络应用（第2版）

站启用匿名访问。

- 更改区域设置：可以更改网站使用的区域设置、时区、排序顺序和时间格式。
- 管理 Web 讨论和通知：可以查看网站的所有 Web 讨论和用户通知，并删除不再需要的任何上述内容。



如果你正在管理子网站，在子网站的“顶级网站管理”页上出现的管理任务是可用于虚拟服务器的顶级网站的管理任务的子集。

“网站设置”和“顶级网站管理”页存储在网站的_layouts 目录中。每个 SharePoint 网站的导航栏都包含一个“网站设置”链接，通过该链接可转到这些网页。即使没有 SharePoint 网站，也可以从兼容的网页编辑器（如 Microsoft Office FrontPage 2003）进入 SharePoint 网站的这些网页，或者通过直接在浏览器中键入这些网页的 URL 进入这些网页。

若要从 Microsoft Office FrontPage 2003 查看这些网页，请在【工具】菜单上单击【服务器】，再单击【管理主页】命令。

“网站设置”页的路径为 `http://websiteurl/_layouts/lcid/settings.aspx`，其中 `lcid` 指的是区域 ID。例如，对于美国英语，`lcid` 为 1033。

“顶级网站管理”页的路径为 `http://websiteurl/_layouts/lcid/webadmin.aspx`。

“网站设置”和“顶级网站管理”页的文件存储在 `..\Program Files\Common Files\Microsoft Shared\Web Server Extensions\60\template\admin\lcid` 文件夹中。

远程使用 HTML 管理页。安装 Windows SharePoint Services 时，将向管理端口安装管理中心页。使用管理端口上的这些网页可以远程管理服务器。你可以从任何客户端打开管理中心页，前提是要知道管理端口号，并使用服务器的管理员组中的成员账户登录。通过使用对某个网站具有“管理网站”权限的网站用户组的成员账户，你可以使用该网站的“顶级网站管理”页。

如果选择在管理端口上使用安全套接字层（SSL），则必须使用 HTTPS 协议才能转至这些网页，通过使用 HTTPS 协议连接管理端口。访问的方法是在浏览器的“地址”框使用 HTTPS 协议并键入服务器管理页的地址，在其中包括安全服务器端口号。

例如，键入 `https://sample.microsoft.com:1439`。

连接到远程“HTML 管理”页时，即可像本地连接一样执行任何管理任务。

2. 命令行管理

在“服务器管理”和“顶级网站管理”页执行的大多数任务也可以在 Windows SharePoint Services 的命令行执行。另外，还可以从命令行设置几个在管理网页无法设置的属性。要使用 `Stsadm.exe` 工具，你必须是服务器计算机的本地管理员组中的成员。因为使用命令行管理方式通常比较少，所以在此不作具体介绍，需要的朋友可以在 Microsoft 网站上查找相关资料。

9.6.2 SharePoint Portal Server 企业门户网站的基本管理

除了以上介绍的门户网站配置方法外，网站管理员还可以对网站用户、网站、数据库服务器和个人网站等进行管理。下面分别予以介绍。

1. 管理网站用户

在 SharePoint Portal Server 企业门户网站主页左边导航栏“动作”栏中单击【管理用户】按钮，打开如图 9-156 所示界面。在其中可以添加、删除网络用户，并且可以修改用户所属的用户组。

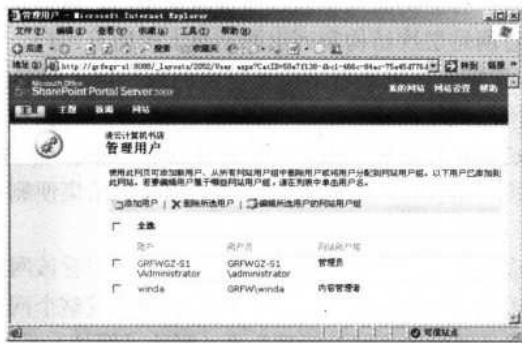


图 9-156 “管理用户”界面

2. 管理网站内容

在 SharePoint Portal Server 企业门户网站主页左边导航栏的“动作”栏中单击【管理内容】按钮，打开如图 9-157 所示界面。在此界面中显示了本网站中的所有库、列表、讨论板和调查。单击库或列表的名称可查看其内容。若要新建库或列表，可在单击相应库或列表名称后打开的界面中单击【创建】按钮，再在打开的界面中创建。



图 9-157 “文档和列表”界面

3. 管理网站和子网站

Microsoft Windows SharePoint Services 中的网站被组织到网站集中。每个网站集具有一个顶级网站。该顶级网站可以具有多个子网站，每个子网站还可以有多个子网站。由于网站在网站集中以层次结构嵌套，因此，管理所有网站是一项有挑战性的工作。

本地服务器管理员和 SharePoint 管理员组的成员可以执行网站集管理员对网站集执行的

任何任务。

可以使用两种方法管理网站和子网站。

1) “HTML 管理” 页

“HTML 管理” 页也就是通过在浏览器中打开网站界面进行，这种管理方式就是比较容易掌握，但功能相对有限。有些功能只能通过顶级网站使用。这些功能包括管理网站集库、查看存储空间分配、查看网站层次结构和列出网站集上的所有用户。

可以使用“HTML 管理” 页来查看网站集以内的或特定子网站的子网站列表。可使用“HTML 管理” 页删除网站或子网站。不同的管理权限级别能够执行不同的操作。本地服务器管理员组成员和 SharePoint 管理员组成员可以从 SharePoint 管理中心删除网站集。网站集管理员还可以使用“顶级网站管理” 页删除网站集。删除网站集便删除了该网站集中的顶级网站和所有子网站。

网站集管理员组的成员可以从“查看网站层次结构” 页查看该网站集中顶级网站之下的所有子网站列表。他们可以删除网站集中的某一特定子网站或整个网站集，方法是从“查看网站层次结构” 页转到该子网站的“网站管理” 页（删除子网站）或顶级网站的“网站管理” 页（删除整个网站集）。

子网站的管理员网站用户组成员只能看到其子网站的下一级子网站。假如子网站之下没有下一级子网站，他们就可以删除他们看到的子网站。

2) 命令行管理

如果使用命令行来管理网站集中的网站，级别将不是重要的，因为始终可以为要管理的网站指定完整的 URL 路径，并可以调整 URL 以列出该网站集中任一级别的网站和子网站。但是，要使用命令行工具，你必须是本地服务器计算机管理员组的成员。

可以通过 Stsadm.exe 命令行工具使用表 9-2 所示的操作来管理网站和子网站。

表 9-2 Stsadm.exe 命令的操作

操 作	说 明
enumsites	列出特定虚拟服务器的所有顶级网站
enumsubwebs	列出特定顶级网站或子网站的所有子网站
renameweb	重命名子网站
deletesite	删除顶级网站和该顶级网站之下的所有子网站
deleteweb	删除子网站。若此子网站中含有其他子网站，则返回一个错误并且不删除该子网站

还可以使用下面的操作来删除网站和子网站：createsite、creatsiteinnewdb 和 createweb。enumsites 和 enumsubwebs 操作使用 url 参数。其语法很简单，只有操作和 URL，下面是示例：

```
stsadm.exe -o enumsites -url <URL>
stsadm.exe -o enumsubwebs -url <URL>
```

enumsites 和 enumsubwebs 操作以 XML 文本的形式提供网站和子网站的列表。例如，运行 enumsites 后生成的网站列表如下：

```
<Sites Count="2">
  <Site URL="http://site_name1" Owner="DOMAIN\userA"/>
  <Site URL="http://site_name2" Owner="DOMAIN\userB"/>
```

```
</Sites>

deletesite 和 deleteweb 操作也是只使用 url 参数并采用相同的语法：

stsadm.exe -o deletesite -url <URL>
stsadm.exe -o deleteweb -url <URL>

renameweb 操作使用 url 和 newname 参数。renameweb 操作的语法如下：

stsadm.exe -o renameweb -url <URL> -newname <new subsite name>
```

9.6.3 门户网站的作业管理

Windows SharePoint Services 中的某些功能依赖于将时间计划好的后台处理。例如，若要能审阅使用率分析信息，则必须先收集该信息（最好是在网站使用负载不是很高时）。使用 Windows SharePoint Services，可以将表 9-3 所示的操作安排在指定时间自动发生。

表 9-3 可以安排在指定时间自动发生的操作

操 作	频 率	作 用 范 围
处理使用率分析日志文件	每日	Web 服务器
发送通知	立即、每日或每周	内容数据库
检查并自动删除未使用的网站	每日、每周或每月	内容数据库
检查指定的公共文件夹中是否有电子邮件附件，并自动将其添加到指定的文档库	每若干分钟、每小时或每日	内容数据库

计划好的时间将应用于特定虚拟服务器上的所有网站。此作用范围决定了作业的运行方式。如果作业的作用范围是 Web 服务器级，则将对每台 Web 服务器计算机运行此作业，而与任何承载相同内容的其他 Web 服务器无关。如果操作的作用范围是内容数据库级，将对内容数据库运行一次此作业，这意味着对整个服务器或服务场中的每个内容数据库运行一次此作业。

Microsoft SharePoint 定时服务是一种后台工具，它负责处理 Windows SharePoint Services 中的计划作业。安装 Windows SharePoint Services 时，此工具安装在 Web 服务器上。SharePoint 定时服务根据公历制订计划。对于计划中的每个作业，必须为该作业指定一个基于 24 小时时钟的开始时间。指定时间时，需要指定本地时间，以及相对于通用协调时间（UCT）的偏移量，并且时间也以这种格式存储。

SharePoint 定时服务使用的数据不存储在上下文中。这意味着，不能将作业计划为每 X 日/周/月/年运行，其中 X 大于 1。因此，虽然你可以计划作业每天、每周或每月运行，但不能计划每两天的过程，如此等等。也不能计划一个月內相对日期的作业，例如每月的第三个星期一。

计划定时作业时，要计划作业的开始时间。例如，可以计划作业每天运行，开始时间在 1:00 AM 和 2:00 AM 之间。应当始终将作业计划为开始于一个时间范围，而不是开始于某个具体的时间。通过此操作，SharePoint 定时服务可以在该范围内的随机时间运行，以便服务器场内的每个服务器不会同时运行计划的作业。例如，如果将使用率分析处理设置在 1:00 AM 至 2:00 AM 的范围内进行，则每个前端 Web 服务器都会在 1:00AM 至 2:00 AM 间的某个时刻开始处理使用率分析。

通过使用 HTML 管理网页可以计划定时作业。若要计划定时作业，请转到包含待计划作

624 网管员必读——网络应用（第2版）

业设置的网页中，再选择希望作业执行的日、月、年和时间。例如，如果将使用率分析处理排在每天 3:00 AM 执行，可使用“配置使用率分析处理”页来指定运行日志处理的时间。

1) 管理通知

由于基于 Windows SharePoint Services 的网站旨在帮助成组用户工作在一起，因此它们会迅速增大，并且会经常更改。对用户来说，要跟上这些更改是非常困难的，特别是在不能每天都登录他们的网站的情况下。为帮助用户与发生在网站上的更改保持同步，Windows SharePoint Services 中包含了一种名为“通知”的功能，这是一种以电子邮件进行通知的服务。当在运行 Windows SharePoint Services 的服务器上创建、修改或删除了文档、列表或列表中的项目时，注册了通知服务的用户将收到通知他们已经发生更改的消息。



在 Microsoft 的 SharePoint Team Services v1.0 中，通知被称为“Web 订阅”，但二者的功能并没有太大差异。

用户可以创建通知来跟踪网站内的项目。

- 列表：用户可收到对列表所作更改的通知，例如在列表中添加、删除或更改项目时。
- 列表项：用户可收到对列表中的特定项目所作更改的通知。
- 文档库：用户可收到对文档库所做更改的通知，例如在文档库中添加、删除或更改文档，或者为文档添加、更改、删除、关闭或激活 Web 讨论时。
- 文档：用户可收到对特定文档所作更改的通知，或者在为文档添加、更改、删除、关闭或激活 Web 讨论时收到通知。



要使通知功能能够用于特定网站，必须先在服务器或虚拟服务器级别上配置电子邮件服务器设置。

用户为这样一个网站创建通知后，他们就可以指定将触发通知的事件类型。只要发生下列情况，就可以生成通知：在文档库或列表中添加、更新或删除文档或列表项时，或者更改了文档或列表的 Web 讨论时。用户可以指定某个这样的事件，或者选择只要在他们需要跟踪的列表、列表项、文档或文档库中发生任何更改时都进行通知。

用户还可以决定他们希望接收通知的频率：即时、每日或每周。即时通知作为单个电子邮件发送，每日或每周通知则组合到整个网站的摘要电子邮件中。

用户可以使用各自网站上“网站设置”页上的【我的有关此网站的通知】链接更改通知。



在 Windows SharePoint Services 中，可自定义通知邮件的内容。请牢记，尽管可以更改邮件的内容，但是不存在识别和提取文档或列表项内实际文本更改的机制。不过你仍然可以自定义邮件中的文本，并对邮件中的字段进行重新排序、添加和删除。只有本地服务器计算机的管理员才能编辑 Windows SharePoint Services 的 XML 模板。

即时、每日和每周通知的邮件文本基于服务器计算机上一系列 XML 模板中的内容。要自定义邮件文本，必须编辑包含该邮件文本的 XML 模板。XML 模板存储在前端 Web 服务器\\Program Files\\Common Files\\Microsoft Shared\\Web Server Extensions\\60\\Template\\LCID\\

XML 目录下，其中 LCID 是区域设置 ID。包含通知的邮件文本的模板如表 9-4 中所述。

表 9-4 包含通知的邮件文本的模板

模板名称	说明	文本和字段中可能包括
notifsitedr.xml	用于每个电子邮件通知的页眉文本	页眉信息（例如网站 URL）、邮件标题信息（例如“每日摘要”或“每周摘要”）和项目信息
notiflisthdr.xml	列表页眉文本	对列表的每日或每周更改的摘要信息
notifitem.xml	事件信息	电子邮件的正文文本，包括文本和占位符“item in list has been changed by name at time”
notifsitedfr.xml	用于每个电子邮件通知的页脚文本	页脚信息，包括字符串“Click here to manage alert settings”



编辑 Windows SharePoint Services 的任何 XML 模板都可能破坏该模板，继而破坏发送通知的机制。请务必编辑模板内的邮件文本，并在需要还原到原始状态的情况下保留原始模板的备份副本。

编辑 XML 模板时，可以将表 9-5 中任意标记包括进来。

表 9-5 XML 模板标记

标 记	说 明
SiteUrl	网站的完整 URL
SiteName	网站的名称
SiteLanguage	网站所用语言的区域设置 ID（LCID）。例如，美国英语为 1033
AlertFrequency	即时（0）、每日（1）或每周（2）
ListUrl	列表的完整 URL
ListName	列表的名称
ItemUrl	项目的完整 URL
ItemName	项目的名称
EventType	ItemAdded（1）、Item Modified（2）、Item Deleted（4）、DiscussionAdded（16）、Discussion Modified（32）、Discussion Deleted（64）、Discussion Closed（128）、Discussion Activated（256）
ModifiedBy	修改项目的用户名称
TimeLastModified	上次修改项目的时间
MySubsUrl	“网站设置”中，指向该网页上“我的通知”的完整 URL



在 XML 模板中，一般是使用数值而不是文本来指定频率和事件类型。因此，如果需要将 AlertFrequency 设置为每周，应该在模板中使用数值 2，而不是键入“每周”。

可以使用任何 XML 编辑工具（如“记事本”）来编辑模板。请牢记，对此邮件文本所作的任何更改都将应用于发送给服务器上所有用户的通知邮件。如果处在服务器场环境下，则必须编辑服务器场中每台服务器上的模板，或者将已编辑的模板复制到服务器场中的每台服务器上。只有本地服务器计算机的管理员才能编辑 Windows SharePoint Services 的 XML 模板。

你可以查看网站或子网站的通知，并删除不再需要的通知。

如果你是服务器管理员或 SharePoint 管理员组的成员，则还可以使用“SharePoint 管理

626 网管员必读——网络应用（第2版）

中心”网页配置通知的如下设置。

- 查看通知设置。
- 打开或关闭通知。
- 指定用户可以创建的通知数。

服务器管理员还可以使用 `Stsadm.exe` 命令行工具配置通知设置。使用命令行可以执行下列操作。

- 打开或关闭通知。
- 指定用户可以创建的通知数。

通知使用 Windows SharePoint Services 电子邮件设置来发送通知项目。配置通知设置时，请务必仔细检查虚拟服务器的电子邮件设置。

2) 设置使用率分析

通过使用率分析可以跟踪服务器上网站的使用情况。使用 HTML 管理网页中的命令，可以配置用于处理使用率日志的设置。在“SharePoint 管理中心”网页中，可以控制下列各项。

■ 是否记录使用率数据。

默认情况下，不启用使用率分析。若要对服务器使用使用率分析功能，则必须启用使用率分析日志记录处理。系统每天都会创建日志文件，以跟踪使用率信息。处理日志文件时，会添加标志来指出日志文件已经过处理，系统不会自动删除日志文件。这些日志文件会保留在下列路径中：`c:\Windows\system32\LogFiles\W3SVCn`，此处的 `n` 是指虚拟服务器的 Internet 信息服务（IIS）实例号（例如，`c:\Windows\system32\LogFiles\W3SVC1`）。如果不想跟踪使用率分析数据以便节约磁盘空间，可以关闭对使用率分析的数据日志记录。

■ 日志文件的存放位置及要创建多少个日志文件。

默认情况下，日志文件存放在 `c:\Windows\system32\LogFiles\STS` 下。在此文件夹中，每个虚拟服务器都有一个文件夹，而在这些文件夹中，每天都有一个文件夹。同时也可以指定你喜欢的其他位置，可以指定系统最多能创建 30 个日志文件。



如果选择其他日志文件位置，则必须确保向 STS_WPG 用户组授予对该目录的“读取”、“写入”和“更新”权限。若没有这些权限，IIS 无法创建或更新使用率日志文件。

■ 是否处理使用率日志，以及处理使用率日志的时间。

默认情况下，日志文件被设置为在 1:00 AM 进行处理。可以计划在更方便的网站停工时间处理使用率日志，也可以指定使用率日志处理的结束时间。例如，如果网站主要由内部员工使用，则可以安排在夜里处理日志，此时对网站的需求低于工作时间。如果有多个服务器，则可以错开处理时间。例如，可以配置处理开始于午夜，并错开 15 分钟，以便 server1 开始于 12:00，server2 开始于 12:15，server3 开始于 12:30，等等。

在 Windows SharePoint Services 中，将从前端 Web 服务器收集使用率分析数据，然后将使用率分析数据收集到临时文件中。每天进行日志处理时，会将数据合并到后端服务器上的内容数据库中。每次将对服务器上的整个网站集收集数据。虽然是在对整个网站集记录并存储数据，但在 HTML 管理网页中查看数据时，只能看到特定网站或子网站的数据，而不是整个网站集的数据。



虽然在“网站集使用率摘要”网页上可以看到网站集的总点击数，但如果要获取详细信息，则必须使用单个网站或子网站的“网站使用率报表”网页。

作为历史记录，在数据库中使用率数据最多可保留三个月。每日信息可存储 31 天，而每月信息可存储 24 个月。

由于使用率分析处理每天只运行一次，所以启用使用率分析处理时，到第二天才能看到数据。日志处理只对一天的有价值数据进行处理。如果将日志处理关闭一周，但打开数据日志记录，则下一次打开处理时，日志处理只处理一天的日志文件。此前所有天的日志文件依然处于未处理状态。

请在“SharePoint 管理中心”网页中控制使用率分析处理的设置，必须是本地服务器计算机的管理员或 SharePoint 管理员组的成员，才能配置使用率分析设置。



为服务器配置使用率分析处理时，此设置将对所有现有虚拟服务器生效。如果此后再添虚拟服务器，则必须再次配置使用率分析处理，才能对新虚拟服务器启用使用率分析。

为服务器配置使用率分析处理的步骤如下。

(1) 在“SharePoint 管理中心”中“组件配置”的“配置使用率分析处理”选项（如图 9-158 所示），打开如图 9-159 所示界面。

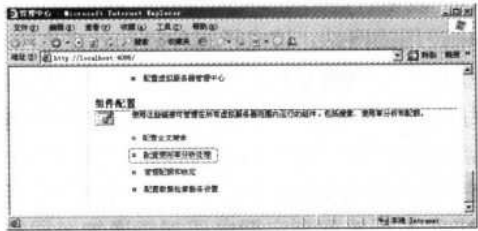


图 9-158 “组件配置”界面下的“配置使用率分析处理”选项



图 9-159 “配置使用率分析处理”界面

(2) 在“日志记录设置”栏中选中“启用日志记录”复选项；在“日志文件位置”文

628 网管员必读——网络应用（第2版）

本框中输入日志文件的存储位置。日志文件的默认位置为 c:\Windows\system32\LogFiles\STS。

（3）在“要创建的日志文件数”文本框中输入介于 1~30 之间的数字。

通常，该数字应是服务器场中数据库服务器数的 1~3，最多可创建 30 个日志文件。

（4）在“处理设置”栏中选中“启用分析处理”复选项。

（5）在“每天运行处理的时间”下，指定启动使用率分析日志处理的时间范围。在“开始时间”框中，选择每天开始运行日志处理的最早时间。在“结束时间”文本框中，选择开始运行日志处理的最晚时间。

（6）单击【确定】按钮使设置生效。

3) 管理未使用的网站

基于 Windows SharePoint Services 的网站可能因为众多原因而变为非活动状态：也许网站是为与已经结束的项目相关的文档设置的，或者是用户当时是为了试验 Windows SharePoint Services 而创建了一个此后不再需要的网站。由于非活动的网站占用服务器上的空间，因此一定要与网站的所有者核对，看他们的网站是仍然需要还是已变成非活动。在 Windows SharePoint Services 中，通过新的管理选项，可以自动向网站的所有者发送通知，要求确认他们的网站是否仍在使用，同时还可以自动删除未经确认的网站。这些功能提供了控制服务器上未使用的网站数量的方法。

网站使用情况确认的原理与用户网站的通知相似。创建网站时，它们将添加到数据库中，并作为活动网站登录。经过一段由管理员定义的时间后，网站的所有者将收到电子邮件通知，询问要重新激活还是删除未使用的网站。该电子邮件通知的文本中包含用于确认网站是否活动或是否要删除该网站的链接。发出通知后，有三种可能的结果。

（1）如果网站在使用中，网站的所有者将确认该网站为活动状态的链接，并保留该网站。当所有者确认链接时，计时器将重新启动，在相同的时间段后，所有者将再次收到通知。

（2）如果网站未在使用，网站的所有者可以按照通知电子邮件中的说明删除该网站，或者什么也不用做。所有者将不断地收到定期电子邮件通知（周期由管理员定义），直到确认网站的使用情况或者网站被删除为止。

（3）如果网站未在使用，且自动删除功能已打开，则网站的所有者将被询问数次（次数由管理员配置），如果不确认使用情况，则网站将自动删除。

自动删除是一种高级管理功能，它可以在不需要管理干预和任何备份机制的情况下删除不需要的网站。为防止在没有任何通知的情况下删除网站，必须在开启自动删除功能之前开启网站使用情况确认功能。另外，在删除网站之前，始终必须向网站的所有者至少发送两次确认通知。除了这些默认包含的基本安全措施之外，还应该考虑下列最佳做法。

■ 要求在创建网站时提供第二联系人。

创建网站的用户会被列为该网站的所有者。根据配置的不同，可能还会要求该用户指定网站的第二联系人。如果有第二联系人的话，确认通知会自动发送给网站的所有者和第二联系人。有关配置“自助式网站创建”的内容已在本章前面有详细介绍，参见即可。

■ 设置进行确认和自动删除之间的合理时间间隔。

例如，如果网站所有者要外出四个星期，而网站定为在四个星期后还未确认即会删除，则在网站的所有者还没有机会进行确认的情况下，该网站就会被删除。如果你要在公司内启

用此功能，请务必在配置确认和删除之间的时间间隔时考虑公司有关度假和缺席的政策。

■ 定期备份网站，以便在意外删除网站时能还原最新的副本。

例如，如果将确认和自动删除配置在每个月的第 15 天发生，则可以制定一个在第 14 天备份服务器的政策。你可以使此过程自动进行，方法是在 SQL Server 中创建一个存储好的进程，用于检查网站的表，并自动备份计划删除的任何项目。

4) 配置网站使用确认和删除

有几种设置可用于进行配置，以控制确认阶段和自动删除阶段之间所间隔的时间。这些设置有以下几方面。

■ 开始发送网站使用确认通知的时间。

初始通知值控制将第一个确认通知发送给新网站，或者已确认正在使用的网站的时间。此值不控制发送通知的频率，只控制在发送初始通知之前等待的天数。

■ 检查需要确认的网站和发出通知的频率。

此频率值影响检查服务器的频率，以及可以发送确认通知的频率。如果将频率设置为每周，则服务器将每周检查一次，且通知也会每周发送一次，即在检查完服务器之后。

■ 执行检查和发送通知的时间。

请根据你的环境更改此时间。例如，如果大多数用户都是联机的，且都在白天单击服务器，则请选择服务器不那么繁忙的夜间时间。

■ 允许自动删除之前发送的通知数。

请调整此数字，确保网站的所有者能在删除网站之前收到通知。通知数还取决于频率，因此如果指定每日检查，且设定为在删除之前有 30 次提醒，则网站所有者将在网站删除前一个月内每天都收到通知。

请确保将这些时间和次数配置为对你的组织环境有用和合理的值。在大的组织内，用户可能需要将数据存储一定的时间，此时可以指定较长的时间间隔（例如，从 180 天前开始发送通知，每个月通知一次，然后在 6 个月都没有得到确认的情况下将网站删除）。如果是为客户承载免费网站，则可能需要缩短这些时间间隔（从 45 天前开始发送通知，每周通知一次然后在 4 个星期后将网站删除）。如果为付费客户承载网站，则不需要使用此功能，除非你拥有可以按需要还原网站的自动备份策略。

表 9-6 列出了所有这些设置（正如“配置网站集使用确认和自动删除”页中所示）以及它们的默认值和最小值。

表 9-6 网站使用确认和删除设置

设 置	默 认 值	最 小 值
在第 ____ 天开始发送通知	90 天	30 天
检查未使用的网站集，按<每日、每周、每月>发送通知，并且在 <时间> 时运行检查	每周	每日
在发送 ____ 次通知后删除网站集	4	按每日时：28 按每周时：4 按每月时：2

在使用上述默认值的一个实例中，第一次通知在 90 天前发出。在前 5 个星期内，每个星期都发送一次通知。在发出初始通知的第 6 个星期时，如果网站的使用情况未能得到确认，

630 网管员必读——网络应用（第2版）

则该网站将被删除。如果网站在任何时间点上确认为在使用中，则计数将重新开始，网站的所有者在 90 天内再也不会收到通知。



如果电子邮件通知因为任何原因而无法排队（如 SMTP 服务器宕机），则计数不会增加。例如，如果已经发送了三次通知，但在接下来要发送第四次通知的那个星期里，SMTP 服务器宕机了，则在这一天不会发送第四次通知，且计数不会增加。在下一个星期再次检查数据库时，第四次通知才会发送出去，且进程从此处继续进行。

确认和自动删除功能依赖于 SharePoint 定时服务对定时作业的执行情况。在此处指定次数和时间间隔时遵循的规则与 Windows SharePoint Services 中其他任何 SharePoint 定时服务作业的都相同。

5) 设置启用了电子邮件的文档库

Windows SharePoint Services 能够将文档库与基于 Exchange 2000 或更高版本的公用文件夹连接起来。任何被附加到公用文件夹内的消息上的文档都可以自动插入文档库，文档库显示文档及发件人地址、主题行和附件插入到文档库的日期和时间（注意，不会保存电子邮件的正文文本。它仍然保留在公用文件夹内，而不会传输到文档库中）。

用户只需发送附加了文档的电子邮件到公用文件夹，文档将自动添加到 SharePoint 网站上的正确文档库中。例如，如果使用 XML 模板存储发票信息，那么，用户可填写 XML 发票后，用电子邮件将它发送到公用文件夹。然后 XML 文件被张贴到文档库，以便累积后产生更大的发票报表，或用于简易检索。

此功能依靠电子邮件传输文档，并使用与所有电子邮件都相同的安全规则。启用此功能前，应注意下列问题 and 弱点。

- 由于电子邮件能跨过防火墙，所以外部用户可用此方法向内部 SharePoint 网站发送文档。这在许多情况下都是有用的，如从外地发回费用报表，但这也可能会使网站向垃圾邮件打开大门。
- 由于电子邮件中的文档可能携带病毒，所以网站可能因为有了带病毒的文档而崩溃。但是从电子邮件附件插入到文档库中的文档可以像文档库中的其他任何文件一样进行病毒扫描。
- 由于电子邮件地址可能是虚假的，所以发件人地址将保存在文档属性中，并在文档库内显示。发件人地址与其他电子邮件地址的可信程度是相等的。
- 若要允许此功能起作用，则文档库应当允许从电子邮件附件匿名插入。你不能控制谁有权向此文档库添加附件文档。但是，你可以用 Exchange 用户管理工具来控制谁能够直接向文档库添加文档，以及谁有权向公用文件夹张贴邮件。
- 与任何公用文件夹或文档库一样，可能会有恶意用户添加太多文档而导致网站或服务器的存储空间被填满，从而使其他用户无法访问网站或服务器。请务必控制有权访问公用文件夹的用户列表，并且考虑用配额控制网站的大小。

此功能遵循对文档库的禁止文件扩展名规则。任何具有在服务器级被禁止的文件扩展名的文档同样会被禁止添加到启用电子邮件的文档库中。例如，如果你有一个扩展名为 .exe 的文件，并且将它发送到公用文件夹，则它不会被传输到文档库。

其工作原理是 SharePoint 定时服务控制何时检查公用文件夹中是否有新的附件文档。SharePoint 定时服务事件运行时，服务将检查公用文件夹中是否有新的文档，并将它们插入到文档库。SharePoint 定时服务仅插入文档，它不会升级、覆盖或删除文档。如果相同文档多次添加到公用文件夹，则该文档还会在文档库中出现多次。但是，文档库中的每个文档都有唯一的文件名（通过添加数字自动生成，如在文件名后加“1”，这样再次添加 filename.doc 时，它将变为 filename1.doc）。

你可以对任何文档库或任何基于文档库模板的列表（如自定义文档库）使用此功能，但此功能不适用于图片库，因为图片库不受支持。与文档一起发送到文档库的数据是固定的。文档被插入时，将忽略在文档库属性中指定的其他任何域，甚至是必需域。

在启用此功能前，必须先将 Exchange Server 公用文件夹配置为能够支持 Windows SharePoint Services。配置此功能后，必须继续从 Exchange 内执行公用文件夹管理任务。

至此本章的内容就全部介绍完了，当然具体配置起来还有许多工作要做，但基本的方法在本章中已作了全面详细的介绍。

